

#Configuration# How to add custom applications to block them using application policy

***Product:** Sangfor NSF

***Version:** Sangfor NSF 8.0.85

*1. Introduction

1.1 User Scenario

Nowadays it's important to have control over the traffic that these protected clients do (even on unwanted applications that the user can use on business assets during work time).

But some applications use well-known ports to operate (for example TeamViewer, Skype, Hide. me, and so on).

If we want to deny this application, it's impossible to apply a firewall rule that blocks a specific port and protocol without causing network issues for clients.

A solution to this scenario is to create a **Custom Application** to permit Sangfor NSF to inspect traffic and block unwanted traffic packets to block specific applications on specific clients within your network.

1.2 Requirements

1. The user's network has Sangfor NSF as a firewall.
2. You must know how the application that you need to block works (type of traffic, ports used, and destinations) to build an identikit on the firewall that permits you to know it and block it.
3. You need to have some clients and applications to block (in this guide we see how to block a custom application that we named test for a specific client that has a static IP)

*2. Configuration Guide

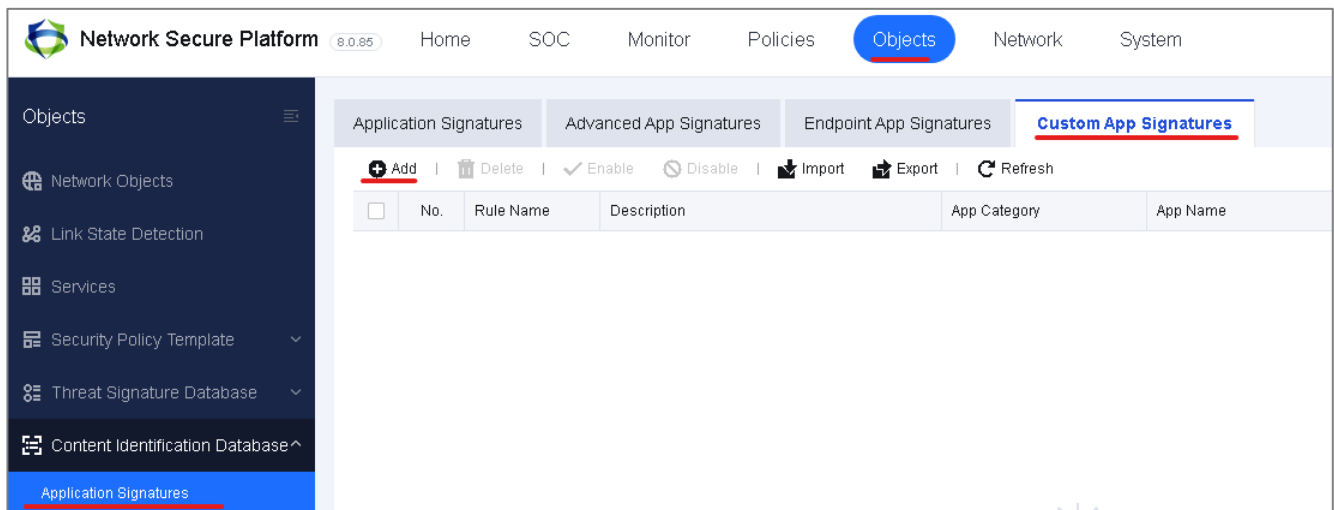
In this guide, we'll see how to create a rule for a specific endpoint to block one custom application.

2.1 Blocking client applications with NSF policy

2.1.1 Create custom application Signatures

We need to add a setting about our custom application that we need to block it on the firewall.

To do so, we can go to the following web ui section:



On this page, we can add a new application signature (on this guide we call it test) that has all the behavior information related to our application that we want to block with NSF (think it as a sort of fingerprint).

Complete the information as it follows:

Add App Signature

☒ Enable

Basic Attributes

Rule Name:

test

Description:

test application information

Category:

Custom_ yourcategory

App Name:

Custom_ test

Packet Feature

Direction:

☒ LAN<->WAN

☐ LAN->WAN

☐ WAN->LAN

This rule only applies to packets transferred in the specified direction.

Protocol:

TCP

Port:

4443

IP Address:

Optional, default: all

Target Domain:

test.com

OK

Cancel

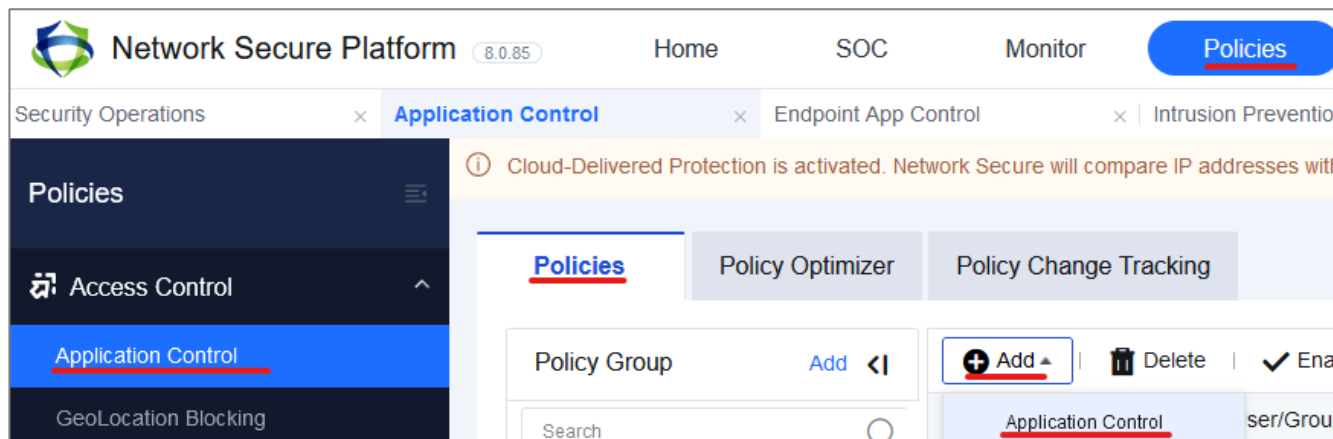
2.1.2 Create application policy

At this point, we need to create an application control policy to filter out packets coming from our

custom test application.

To achieve this, you must go to this section of NSF's web ui and choose to create an Application Control policy:

Policies -> Application Control -> Policies -> Add



On the new policy, we need to choose a policy group and position to ensure that this policy works as expected (for example, we set the default-policy group policy).

During application policy creation, when you select the corresponding src. Address voice, you can create a network object that identifies the client which you want to block custom test application.

Add Application Control Policy

Basics

Name: Block custom test application

Status: ☒ Enabled ☐ Disabled

Description: Optional

Policy Group: 7.default-policygroup

Position: Above Policy name

Tags: Optional

Source

Src Zone: any

Src Address: ☒ Network Objects ☐ MAC Address

Test client

User/Group: /

In this guide, I add a single IP related on a specific client:

Select Network Object

Available (27) | [Add](#) ^

<input type="checkbox"/>	Name	<u>Address</u>
<input type="checkbox"/>	All	Address Group
<input type="checkbox"/>	CODE LINK	Domain Name

Edit Address

Type: ☒ IP Address ☐ Business Asset Address

Basics

Name:

Test client

Description:

block test application

Address Group:

Optional

In Use:

In use

IP Address

Protocol: ☒ IPv4 ☐ IPv6

IP Address:

10.0.0.62

DNS Lookup

After adding this information, you can click save and select this client on previous menu about new policy creation.

At this point it's important to specify the destination about the application traffic that we want to block and the custom application we created before

Edit Application Control Policy

Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Policy Group:

Tags:

Source

Src Zone:

Src Address: ☒ Network Objects ☐ MAC Address

User/Group:

Destination

Dst Zone:

Dst Address: ☒ Network Objects ☐ MAC Address

Services:

Applications:

Others

Action: ☐ Allow ☒ Deny

On the above screenshot click on applications and select the newly created applications on previous step and click save.

Add Application Control Policy

Basics

Name:

Block custom test application

Status:

Enabled

Disabled

Description:

Optional

Policy Group:

7.default-policygroup

Position:

Above

Policy name

Tags:

Source

Src Zone:

Src Address:

User/Group:

Destination

Dst Zone:

DstAddress:

Services:

Applications:

Select

Available (4635)

Selected (1)

Education-Learn

Book-Encyclopedia

Shopping

Artificial_Intelligence

SSL Data

News-Media

HTTP_POST

Travel-Traffic

Internet Finance

Job-Search

Custom_yourcategory

Custom_test

Custom_yourcategory

Save

Cancel

Save and Copy

Save

Cancel

Now on the bottom of this page, we define the behavior of our policy and a schedule (if needed)

Add Application Control Policy

Position:

Above

▼

Policy name

▼

Tags:

Optional

▼

Source

Src Zone:

any

▼

Src Address:

☒ Network Objects
 ☐ MAC Address

Test client

⋮

User/Group:

/

⋮

Destination

Dst Zone:

any

▼

DstAddress:

☒ Network Objects
 ☐ MAC Address

All

⋮

Services:

any

▼

Applications:

Custom_yourcategory

▼

Others

Action:

☐ Allow
 ☒ Deny

Schedule:

all-week

▼

Advanced:

Settings

Save and Copy

Save

Cancel

Now click save to complete the policy creation.

Now you can see if there are some hits about newly created policy.

Name	Tags	Src Zone	Src Address	User/Group	Dst Zone	Dst Address	Services	Applications	Schedule	Action	Hit
olicygroup (2)											
Block custom test application	-	any	Test client	/	any	All	any	Custom_y...	all-week	Deny	0
default-policy	-	any	All	All	any	All	any	All	all-week	Deny	97

*3. Precaution

Keep in mind that if you have some DHCP clients, I suggest you create a network object related to a specific network instead.