Stormshield Network Security Workshop Guide

Microsoft Azure Test Drive

Version 1.0 – August 2017

CONTENTS

About this guide

The activities described in this guide will walk you through the *Stormshield Network Security* (hereafter: SNS) interfaces to achieve a typical network protection scenario.

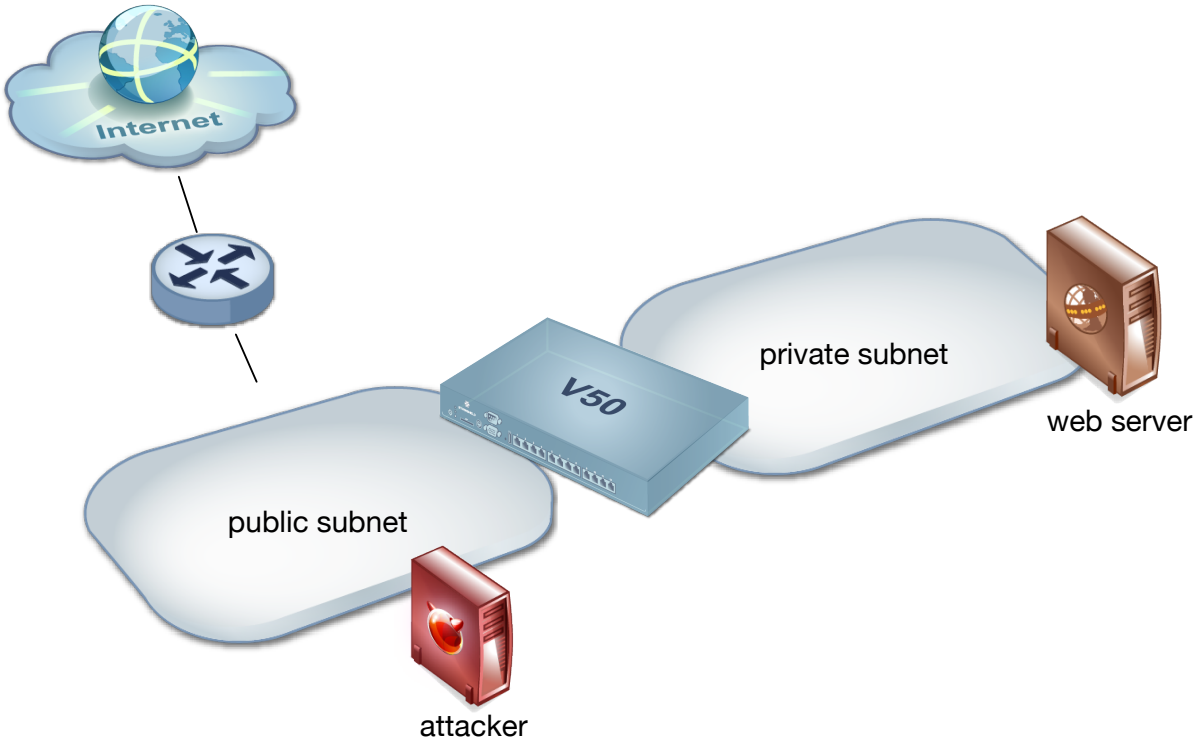
You will learn how to use SNS to protect a web server against incoming malicious traffic.

Environment

The provided environment consists of:

- An SNS V50 appliance, connecting both private and public subnets
- A web server located on the private subnet
- An attacker machine located on the public subnet

All incoming traffic to the web server is going through SNS.



Step 0: Launch the test drive

Follow the test drive launch procedure to obtain:

- The appliance IP address and name (FQDN) and credentials
- The attacker VM IP address and name (FQDN)
- The protected web application FQDN

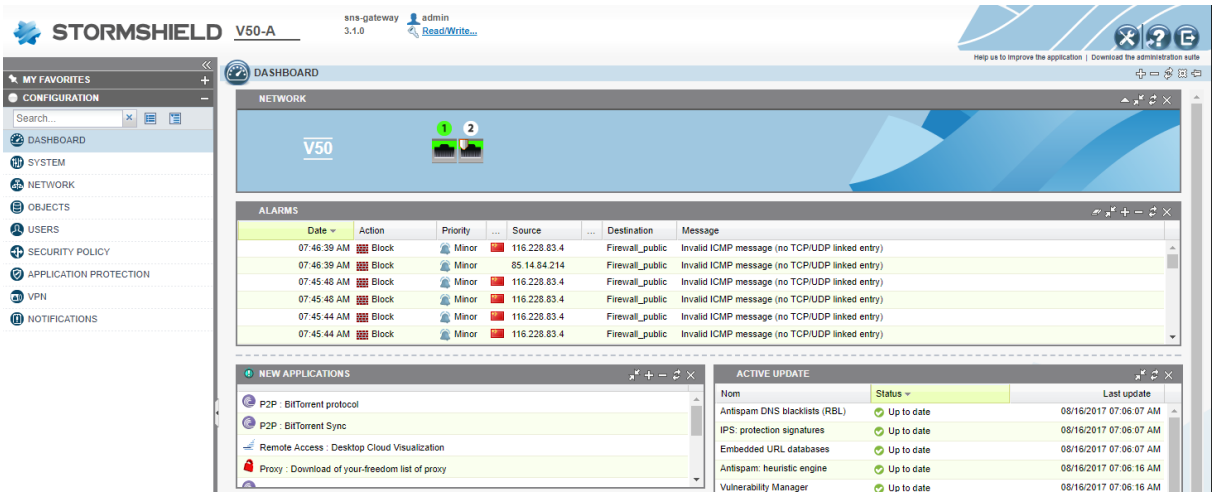
You will need this information for later activities.

Step 1: Configure the appliance through its Web Interface

Log on to the Web Interface

Open a new tab on your web browser and enter the SNS web admin URL. Use the *admin* login and the password provided in the Access Information.

Once logged in you are directed to the main dashboard which provides information about the appliance state and the last events. The configuration menu is on the left.



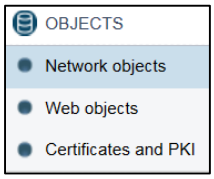
Check Filtering Rules

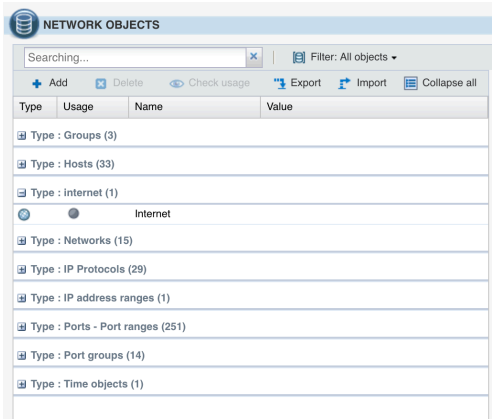
Review:

- Objects
- Filtering rules
- Applications and protections

Objects

Network objects are available for review and configuration from the left-hand side menu:



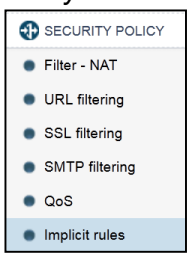


Stormshield firewalls do not use straight IP or network addresses in the filtering rules but use aliases instead, called *objects*. Each time you want to add a new address, the object database is automatically invoked, allowing you to create new objects as required.

Filtering Rules

Through filtering policies, administrators can define rules to allow or block traffic going through the Stormshield UTM. Depending on the type of traffic, security inspection criteria can be defined and enabled for antivirus scan, antispam scan, URL filtering, etc.

Filtering rules are found in the *Security Policy* menu:



Filtering rules can be based on:

- Source and/or destination IP addresses, network addresses, or host names (FQDN)
- Reputation and geographical location of a host
- Incoming or outgoing traffic
- The value of the DSCP field
- The TCP/UDP service in use
- The type of IP-based protocol in use, including ICMP types
- Users or groups requiring authentication

Stormshield firewalls use *Stateful Packet Inspection* (SPI) to memorize connection states for TCP, UDP, and ICMP in order to detect potential anomalies or attacks. Traffic detected by a filtering rule in one direction will also take into account replies that are part of the same connection and will be implicitly allowed. There is no need to define rules to allow response packets for authorized traffic.

There are ten available slots to store your filtering rules, with only one active slot. Slots act like ten different possibilities to back up your configurations, allowing to easily switch back and forth in a single click to designate the active slot.

For the Test Drive a predefined slot has been created and activated: Azure – Test Drive

FILTER - NAT

(9) Azure Test-drive | Activate this policy | Edit

FILTERING | NAT

Searched text | New rule | Delete | Up | Down | Expand all | Collapse all | Cut | Copy | Paste | Reset rules statistics | Reset colun

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comment
Administration (contains 3 rules, from 1 to 3)									
1		on	pass	Any interface: public	Any	bootpc		IPS	agent dhcp on out
2		on	pass	Any interface: public	Firewall_public	ssh		IPS	ssh on out
3		on	pass	Any interface: public	Firewall_public	Any	icmp	IPS	allow ping on public interface
RDR to web server (contains 1 rules, from 4 to 4)									
4		on	pass	Any interface: public	Firewall_public → web-server	http		IPS	rdr to web server
Private to Internet (contains 1 rules, from 5 to 5)									
5		on	pass	Network_private	Any	Any		IPS	private to internet
Block all (contains 1 rules, from 6 to 6)									
6		on	block	Any	Any	Any		IPS	

URL Filtering

Stormshield UTM offers URL filtering, SMTP filtering, anti-spam, and anti-virus scans. URL filtering can be found under *Security Policy*:

SECURITY POLICY
- Filter - NAT
- URL filtering
- SSL filtering
- SMTP filtering

URL FILTERING

(1) default01 | Edit | Add rules by category | URL database provider: Extended Web Control

Add | Delete | Up | Down | Cut | Copy | Paste | Check URL classification | Classify

	Status	Action	URL category	Comments
1	Enabled	Pass	Unknown	
2	Enabled	Pass	Advertisements & Pop-Ups	
3	Enabled	Pass	Alcohol & Tobacco	
4	Enabled	Pass	Anonymizers	
5	Enabled	Pass	Arts	
6	Enabled	Pass	Business	
7	Enabled	Pass	Transportation	
8	Enabled	Pass	Chat	
9	Enabled	Pass	Forums & Newsgroups	
10	Enabled	Pass	Compromised	
11	Enabled	Pass	Computers & Technology	
12	Enabled	Pass	Criminal Activity	
13	Enabled	Pass	Dating & Personals	
14	Enabled	Pass	Download Sites	
15	Enabled	Pass	Education	
16	Enabled	Pass	Entertainment	
17	Enabled	Pass	Finance	
18	Enabled	Pass	Gambling	

For policy creation, you just need to know the source of a connection, the destination and the type of analysis that you want to do.

Application Protection
Stormshield UTM also offers protection against a very large variety of known protocol attacks. These are defined and activated under *Application Protection*. Here are for example some protection rules against known errors found in the HTTP protocol:

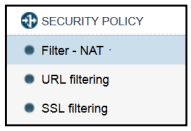
Invalid %u encoding char in URL	Block	Major	http:47
Evasion using %u encoding char encoded URL	Block	Major	http:48
Invalid escaped char in URL	Block	Major	http:49
Escaped NULL char in URL	Block	Major	http:50
Escaped Percent char in URL	Block	Major	http:51
Evasion using UTF-8 encoding	Block	Major	http:52
Invalid HTTP protocol	Block	Major	http:53
Possible buffer overflow on URL	Block	Major	http:54
Possible buffer overflow in HTTP request/reply	Block	Major	http:55
Tunnelling using CONNECT method	Block	Major	http:56
Multiple slash in URL	Allow	Ignore	http:78
Directory self reference	Block	Minor	http:79
Directory traversal	Block	Major	http:80
Bad UTF-8 encoding in URL	Allow	Minor	http:82

There are multiple possibilities to configure the application protection. Protection profiles can also be selectively applied to different networks or users.

Add a re-direction to the web app server

For the test environment, we want all incoming traffic to be re-directed to the web server through the Stormshield appliance. This will place the Stormshield UTM in the way of incoming attacker traffic.

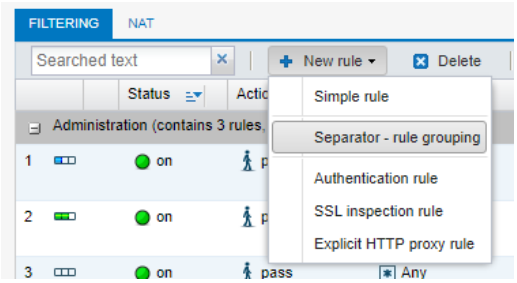
Add a re-direction rule to the web server with a NAT re-direction. NAT rules are found under *Security Policy*:



Re-direct all incoming *http* traffic on the *Firewall_public* IP address to the internal web server, for which a host object is already created.

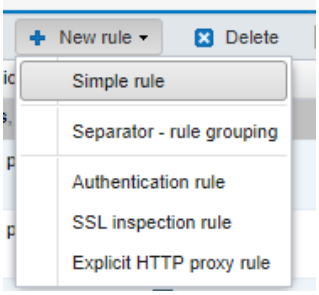
You can use separators to group policies to make them easier to read.

In the grid select *Private to Internet* and click on *New rule / Separator* to insert a new rule group.



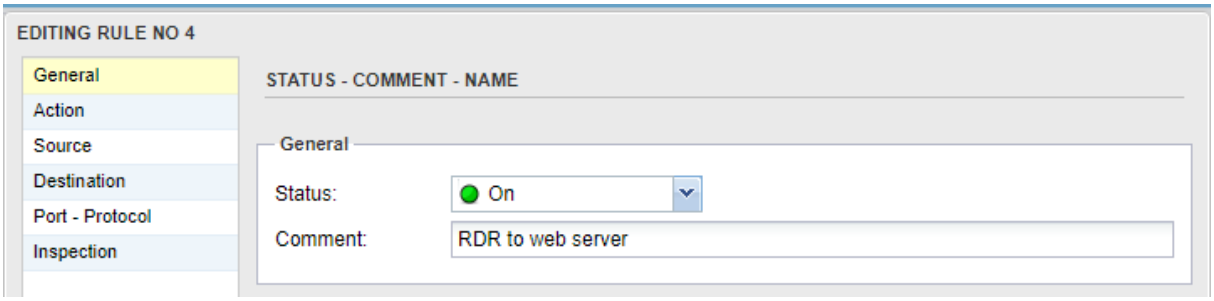
Name the separator *RDR to web server*.

Click on *New rule / Simple rule* to insert a new filtering rule below the new separator.

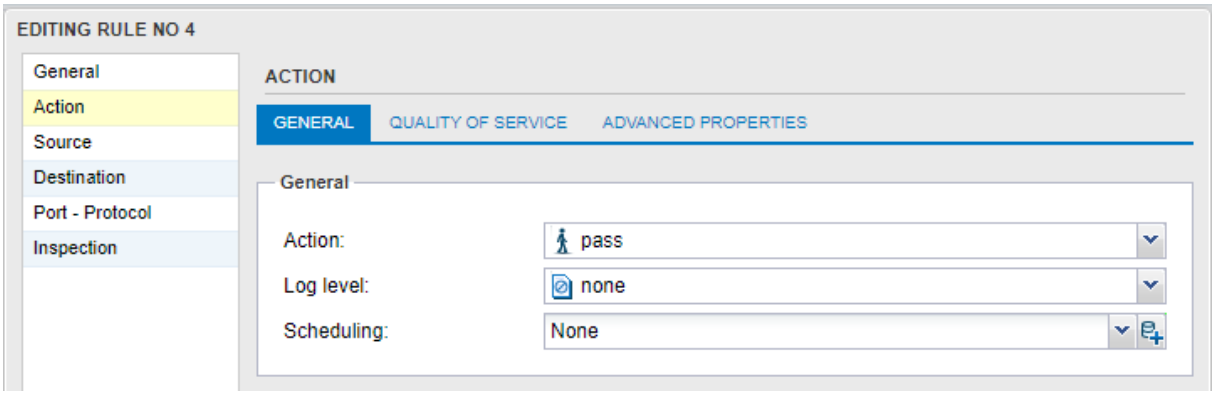


Double-click on the rule number (4) to edit the rule properties.

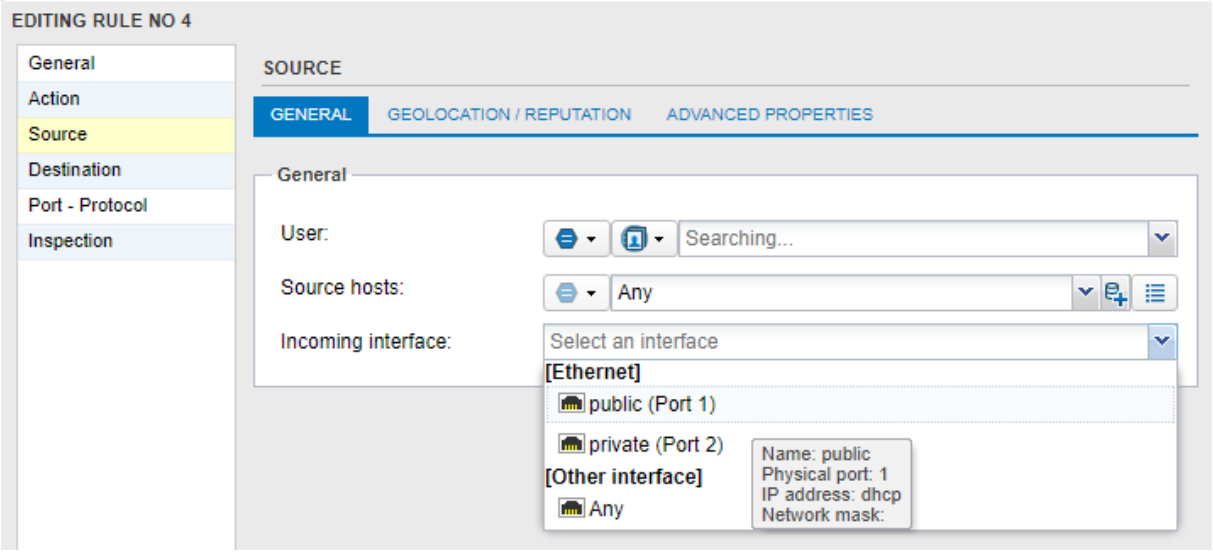
On the *General* tab, you can set the status to *On* and edit the comment.



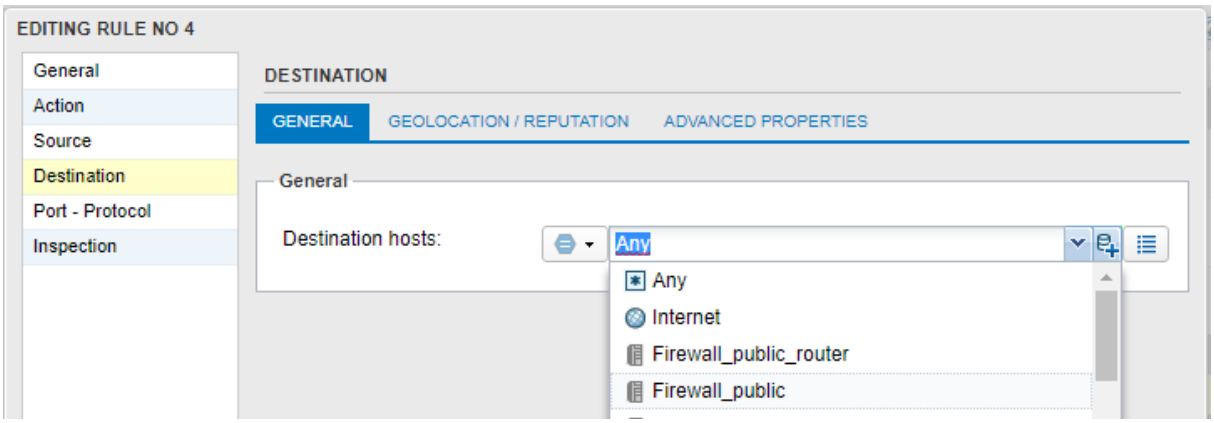
On the *Action* tab, set the action to *Pass*.



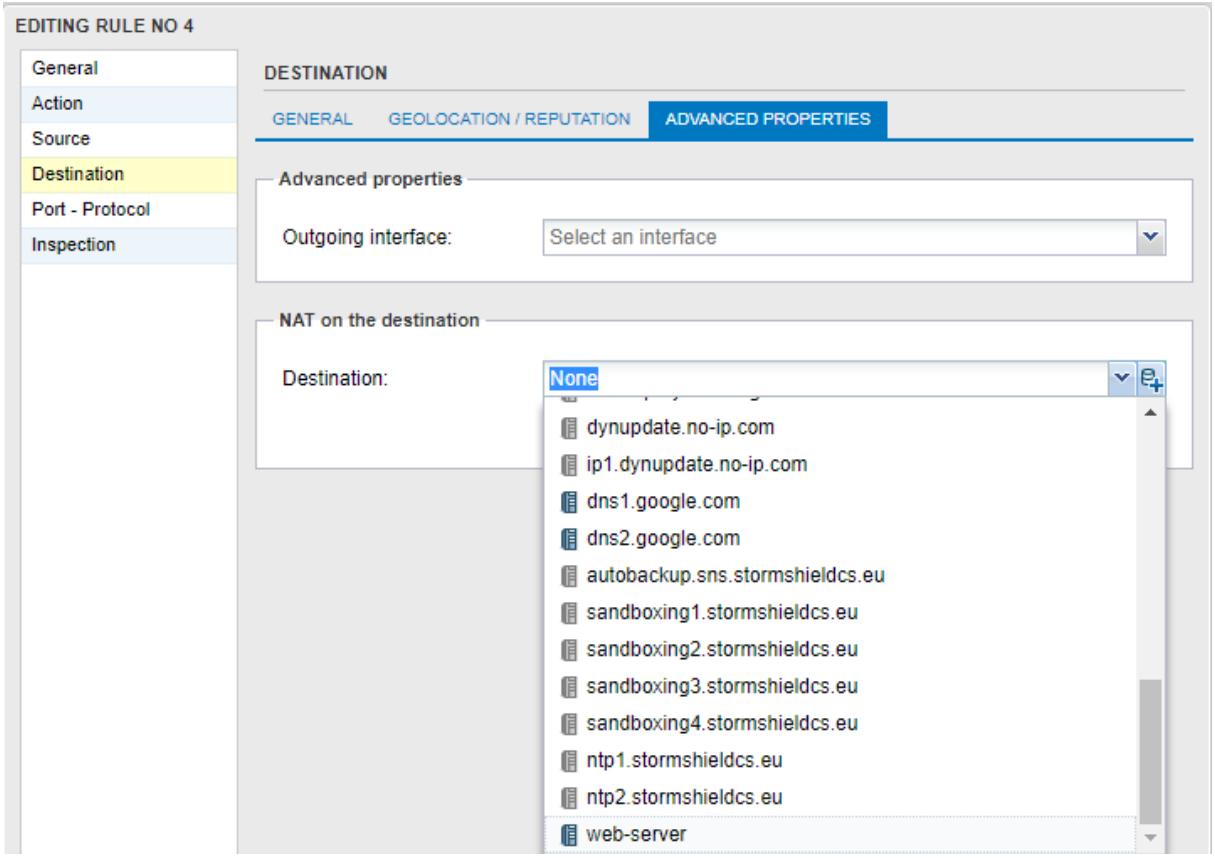
On the *Source* tab, select *public* as incoming interface.



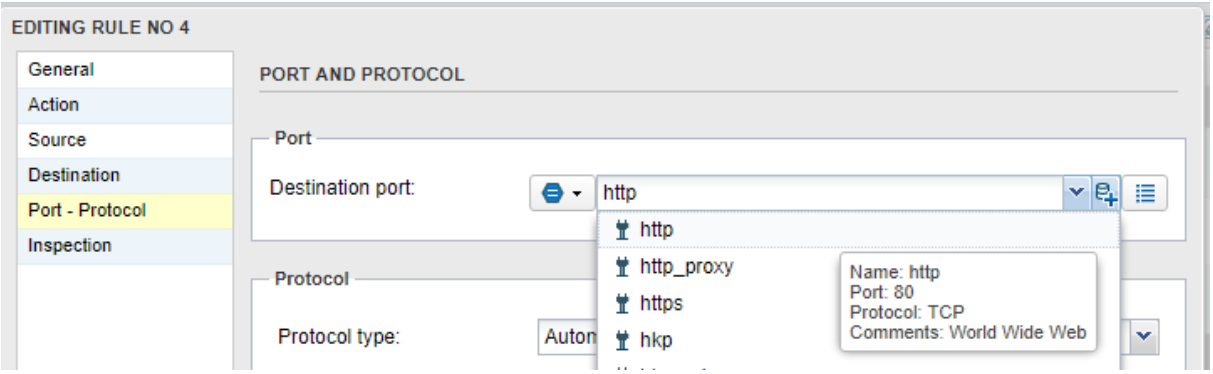
On the *Destination* tab, select *Firewall_public* as Destination Host.



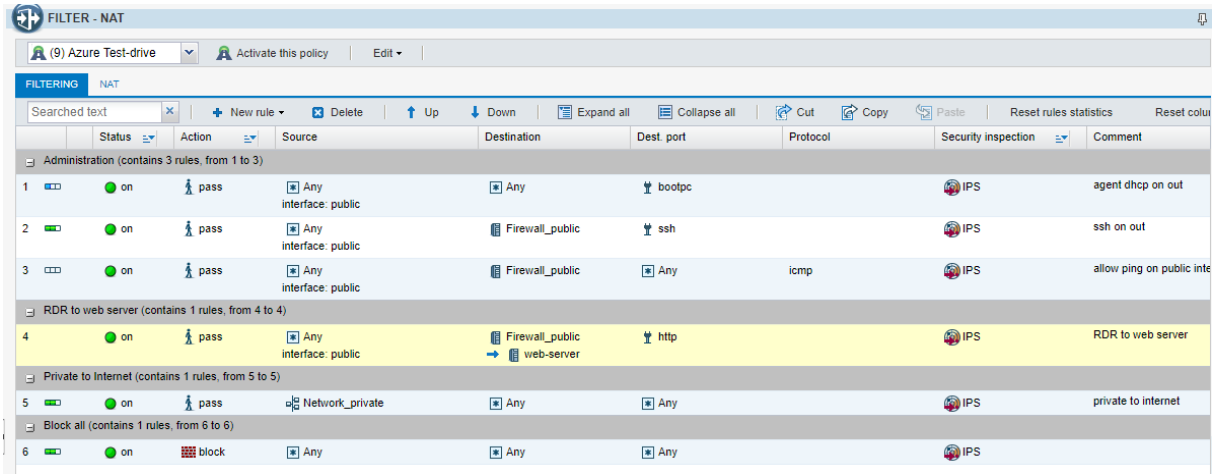
In *Advanced properties*, select the *web-server* host in the NAT as destination field.



On the *Port – Protocol* tab, select *http* as destination port.



Click *OK* to validate the rule.

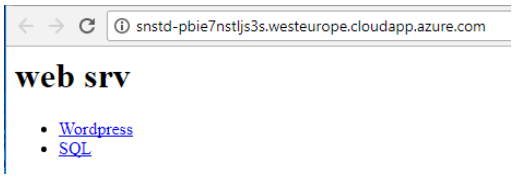


Click *Save and apply* to apply the updated filtering slot.

The highlighted filter/NAT rule means: all traffic arriving from the public interface and directed to the public IP address of the firewall on port 80 is redirected to the internal web-server.

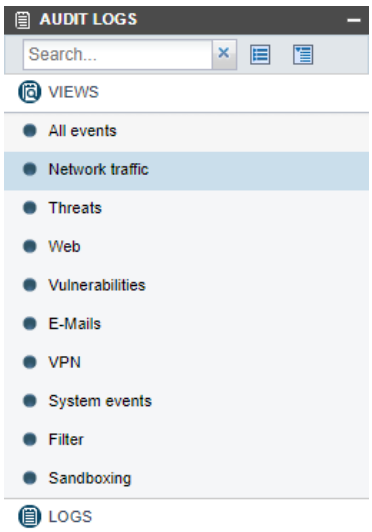
Let's check that the rule is correctly set and the web server is reachable.

Open a new tab in your web browser and enter the protected app URL as provided in the Access Information. You should see the app menu.



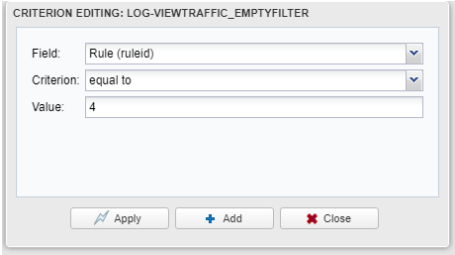
Click on the WordPress link in order to generate traffic to the server.

Go back to the SNS web admin tab and go to the reporting:
Audit logs / Views / Network traffic

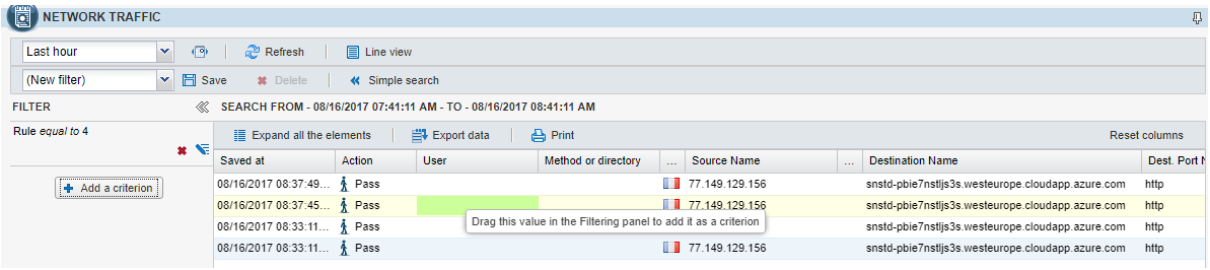


Stormshield firewalls provide advanced reporting in order to have a clear view of all traffic and detected attacks. Let's single out re-directed traffic:

Select *Advanced search*, click *Add a criterion*, select *Rule (ruleid)* and set it to 4 as this is the RDR rule number you previously created.



Click *Apply*: only connections matching this filtering rule are displayed.



Step 2: Take the attacker role

Launch a brute force attack

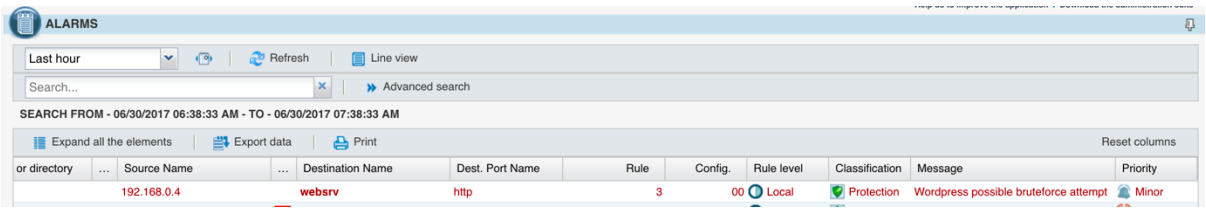
You will now test protection against a simple brute force attack.
To launch the attack, let's simulate the attacker machine and exploit the server.

In a new web browser tab, enter the attacker URL as provided in the Access Information and click *Launch attack*.

This should end with `Communication error`, indicating the attack failed.

Check Alarm Logs

From the SNS web admin, go to:
Audit Logs / Logs / Alarms
and look for the event: *WordPress possible brute force attempt has been blocked*.



Launch an SQL injection attack

Another kind of attack that we can test is an SQL injection.
The idea behind the SQL Injection attack is to modify the SQL query in order to manipulate the remote server.

A typical SQL query could be:

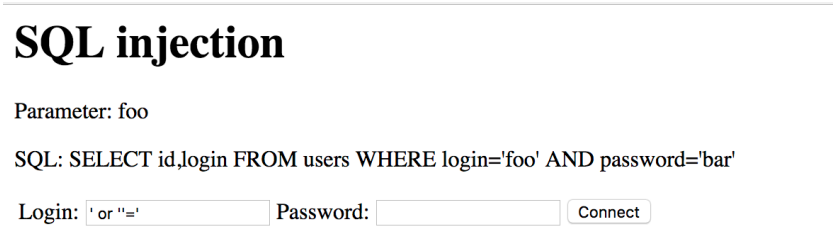
```
SELECT id,login FROM users WHERE login='foo' AND password='bar'
```

The aim of this attack is to validate the Select even when we do not know login or password.
This can be achieved by adding a OR statement with a condition which is always true.
The query becomes something like:

```
SELECT id,login FROM users WHERE login='foo' OR 1=1 AND password='bar' OR 1=1
```

Let's try:
In a new web browser tab, enter the protected app URL as provided in Access Information and click *SQL*.

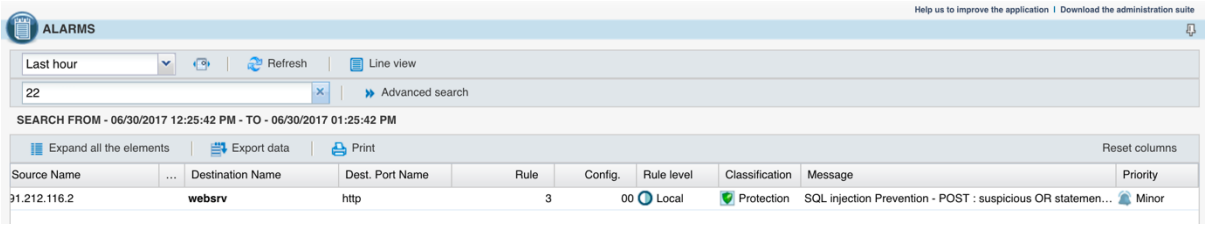
Use the string `' or ''='`
for both login and password and click *Connect*.



You should be logged as the *admin* user:

Check Alarm Logs

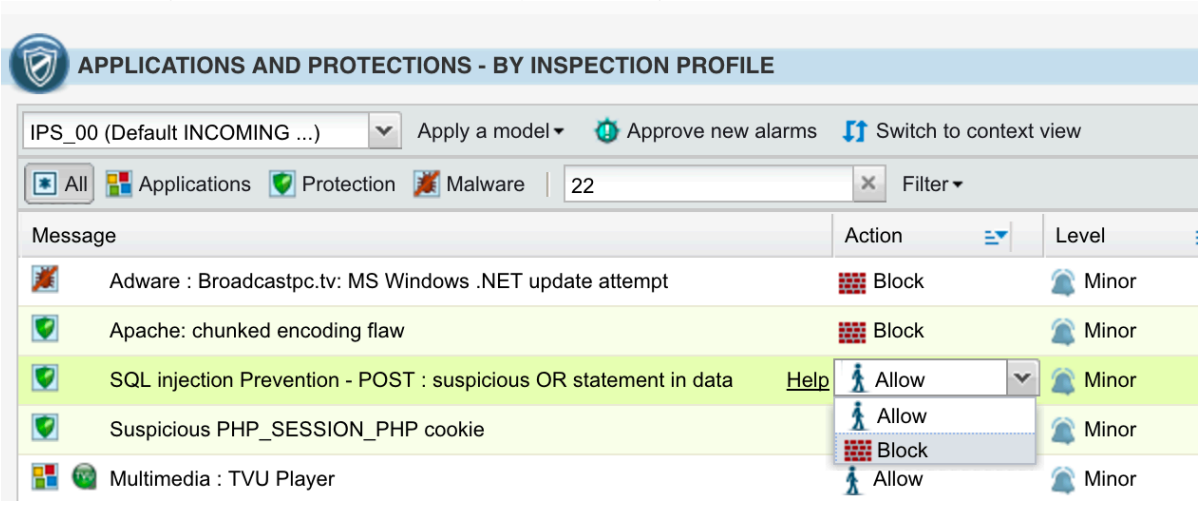
Go back to the SNS web admin tab and go to
Audit Logs / Logs / Alarms
you should see the *SQL injection Prevention* event.



Step 3: Protect your web server

Change the Alarm Action

Go to *Configuration / Applications and Protections*, select the **IPS_00** profile, which is the default profile for all the incoming traffic. Search for the **http:client:data** context, select alarm 22 and change the action to *Block*. Apply the configuration.



Attack Again

Now that the alarm is set to block it is no longer possible to exploit the page and to obtain administrator access.

Let's check:
Browse again to the SQL injection attack page and launch the attack. This time the page should not even load.
In the alarms log, the same event is now blocked.