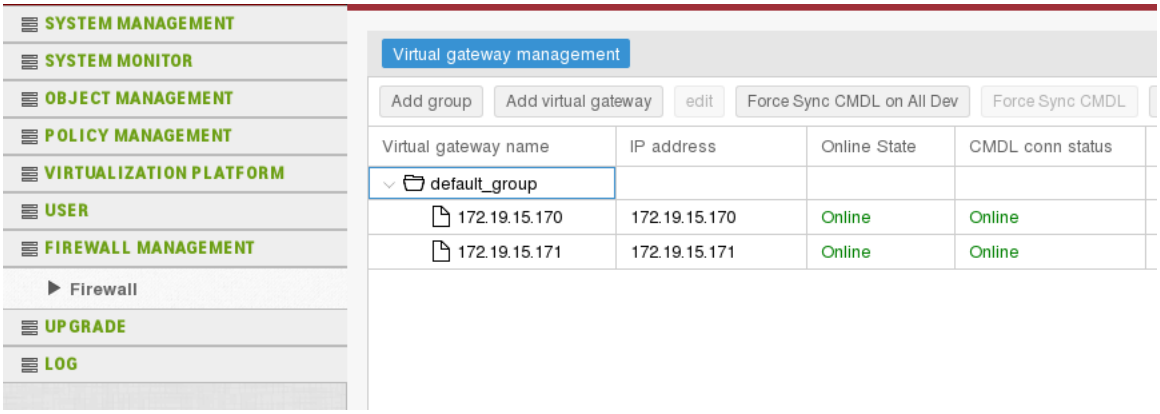
Support Doc

1 Troubleshooting (logs, procedures and techniques)

Troubleshooting commands (show/debug/GUI), example of command output and what to look for

An SVM has two connection-status fields on the service manager (*the first one 'Online State' is hidden since vDFW-N-1.0.6*). Each status field stands for a channel of communication. One channel is for special configuration and the other is for all other communications between the service manager and the SVM.



Detail of the two fileds:

1. An SVM listens on tcp port 4000 to receive special configuration from the service manager. The special configuration mainly contains the address of the service manager. It's in case that the address of the service manager is changed when the SVM is running.

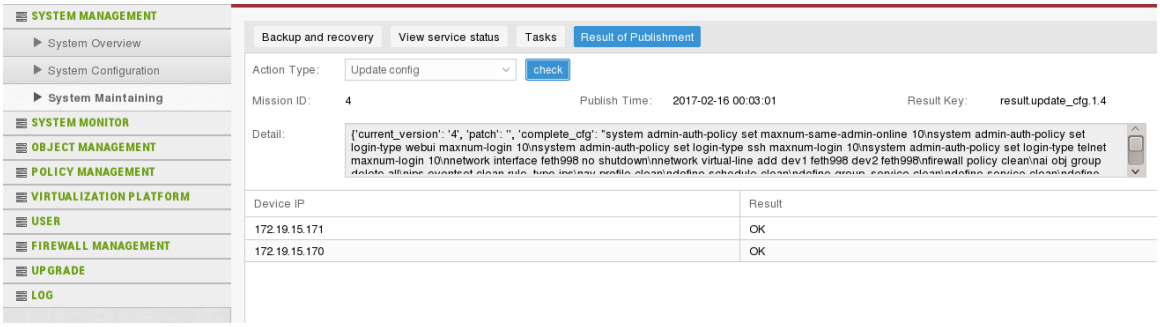
2. The service manager runs a Redis server to publish policies and settings, and send messages to SVMs. The service manager checks the client list of the Redis server to see whether an SVM is online for every N (N=10 in vDFW-N-1.0.6) seconds.

To resolve:

If ererything is OK, both fields should be "online". If the second status (CMDL)

shows "offline", user can select that device and click the button "Force Sync CMDL" and wait the status to become "online".

User can check the result of the last configuration publishment. Every SVM is expected to do things and write result to the Redis server. The result of a SVM should be OK if it works fine, otherwise there will be an error message.



Troubleshoot if the traffic is being redirected from ESXi.

Show slots under vnics:

 # summarize-dvfilter

There should be a slot with number >= 4 under the protected vnic. This command also shows the filter name.

```
world 18361993 vmm0:CentOS-7-fake_agent vcUuid:'50 02 a5 5a 0f f2 d8 d4-0a 8d 85 c5 67 e8 f0 1a'
 port 33554441 CentOS-7-fake_agent
  vNic slot 2
   name: nic-18361993-eth0-vmware-sfw.2
   agentName: vmware-sfw
   state: IOChain Attached
   vmState: Detached
   failurePolicy: failClosed
   slowPathID: none
   filter source: Dynamic Filter Creation
  vNic slot 4
   name: nic-18361993-eth0-serviceinstance-39.4
   agentName: serviceinstance-39
   state: IOChain Attached
   vmState: Attached
   failurePolicy: failOpen
   slowPathID: 519
   filter source: Dynamic Filter Creation
```

The filter name can also be listed with this command:

 # vsipioctl getfilters

```
Filter Name                : nic-18361993-eth0-serviceinstance-39.4
VM UUID                    : 50 02 a5 5a 0f f2 d8 d4-0a 8d 85 c5 67 e8 f0 1a
VNIC Index                 : 0
Service Profile            : serviceprofile-37
Filter Hash                : 63839
Flow Collection Flags
   L2 Pass Flows           : On
   L2 Drop Flows           : On
   L3 Drop Flows           : On
   L3 Inactive Flows       : On
   L3 Active Flows         : On
   All Flows               : Off
   Global override         : On
```

Show rules of a filter:

 # vsipioctl getrules –f <FILTER_NAME>

```
ruleset 25890 {
  # Filter rules
  rule 25891 at 1 inout inet protocol any from any to any punt;
}
```

Troubleshoot if the traffic is being redirected from SVM.

Login to the firewall management console in SVM:

 # /tos/bin/login

username: **superman**

password: **talent**

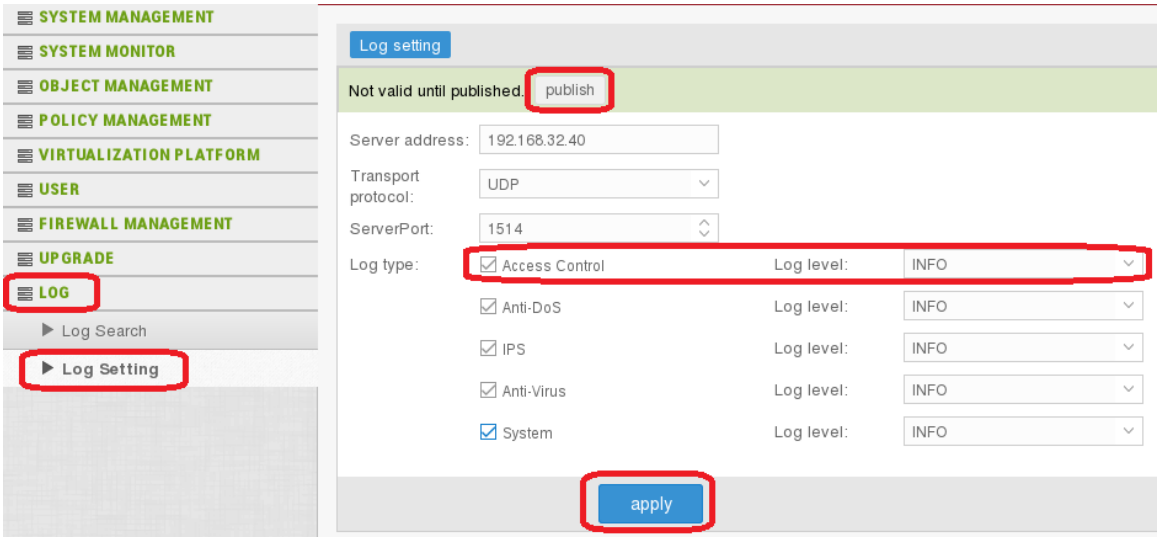
Then call *system tcpdump* to capture packets. This will show only the redirected packets.

```
TopsecOS# system tcpdump -nn -i any host 172.19.15.180 -q
ngtos_tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 65535 bytes
R-0  [feth998] 02:08:15.484348 IP 192.168.32.36 > 172.19.15.180: ICMP echo request, id 30743, seq 1, length 64
X-0  [feth998] 02:08:15.484485 IP 192.168.32.36 > 172.19.15.180: ICMP echo request, id 30743, seq 1, length 64
R-0  [feth998] 02:08:15.485082 IP 172.19.15.180 > 192.168.32.36: ICMP echo reply, id 30743, seq 1, length 64
X-0  [feth998] 02:08:15.485113 IP 172.19.15.180 > 192.168.32.36: ICMP echo reply, id 30743, seq 1, length 64
```

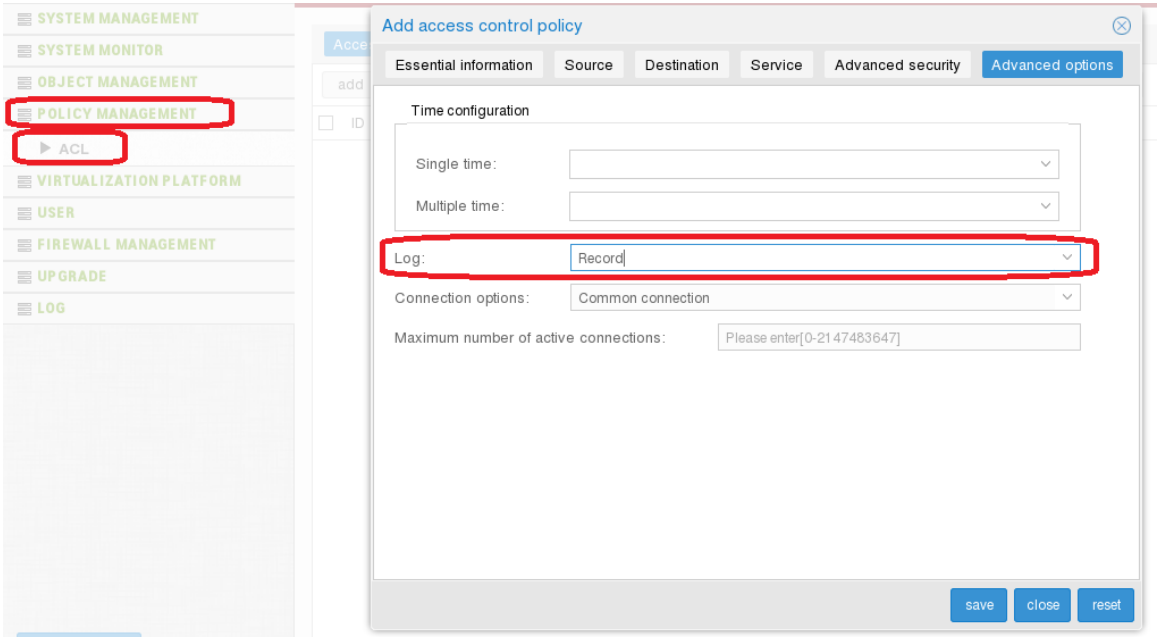
Troubleshoot if the traffic is being redirected from the service manager.

User can check logs to see whether the access control policy worked.

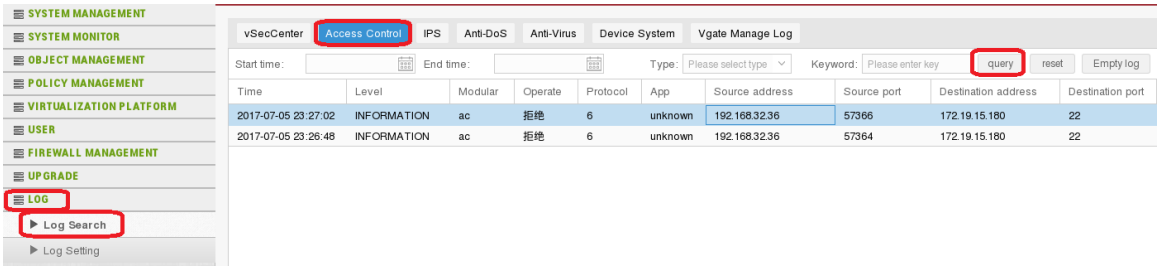
Configure log settings of SVMs. Check the Access Control and set its level to INFO:



Turn on the log recording in the access control policy:



Generate network traffic matching the access control policy, the SVM will send logs to the service manager. User can check SVM logs on web-UI of the service manager:



2 Steps to collect logs from partner SVM

Where to find the log for each component?

Service Manager Log

/var/www/vSecCenter/logs/*.log

/var/log/redis/*.log

SVM Log

Common logs of the firewall will be sent to the service manager. User can browse logs of both the service manager and the SVMs on UI of the service manager.

3 Steps to upgrade from previous partner solution versions

Upgrade procedure, upgrade path, impact to data plane traffic

Upgrade SVM

Upload firewall upgrading package to the service manager, then publish the package to SVMs.

When upgrading, the firewall processes in the SVM will restart, and the firewall policies won't work during that time. Currently, the default failure policy is fail-open, so the data plane traffic will bypass.

Upgrade Service Manager

1. Login to the service manager's terminal.

2. Stop the services.

3. Upgrade with RPM packages provided by Topsec.

4. Start the services.

4 Sample problematic scenarios and how to address them

4.1 Most common misconfigurations

Forget to set the services to be auto-started.

The services in the service manager is not auto-started by default. Administrator can execute **vseccenter.sh autostart** to let it start after booting.

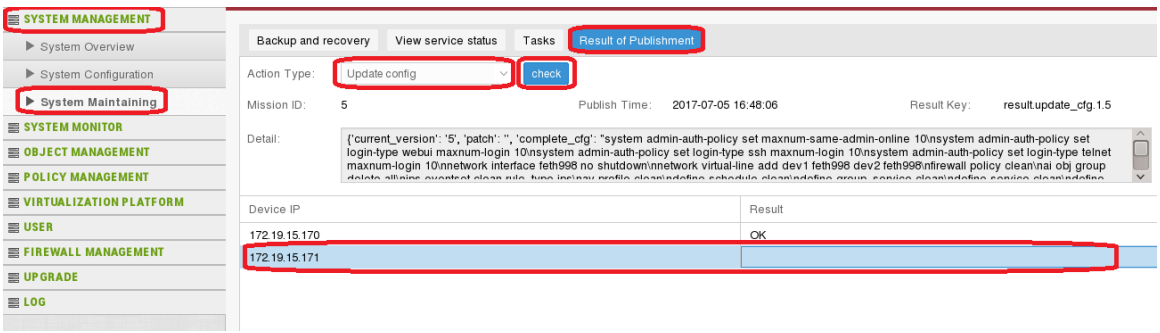
Forget to publish changes.

User should click “publish” button to publish firewall policies and settings to the SVMs. Otherwise they will not be valid.

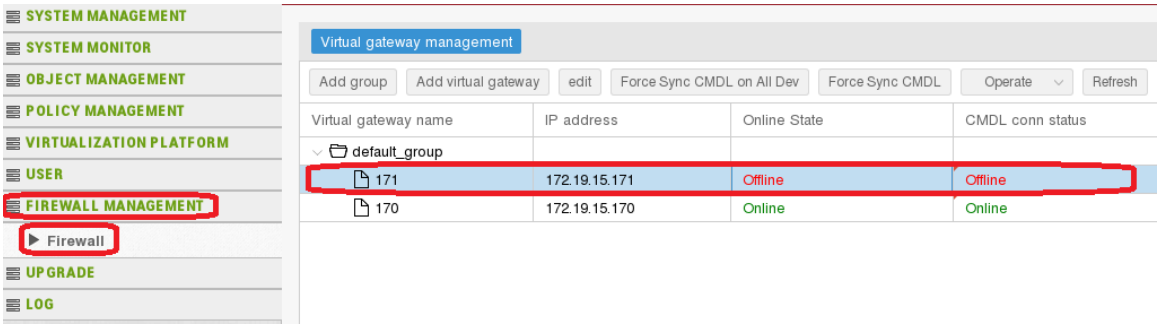
4.2 Troubleshoot a sample error

Troubleshoot a Sample Error

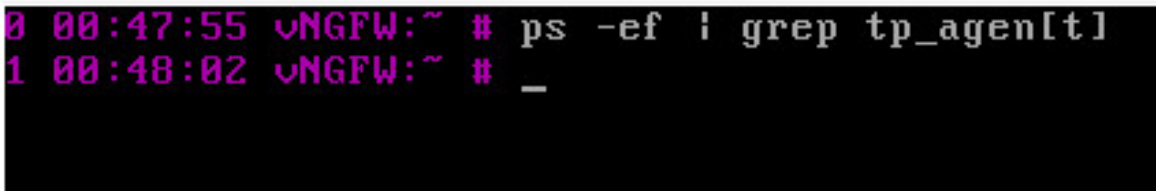
Published access control policy, but it doesn’t work. Check the result of the publishment, find that one SVM didn’t response:



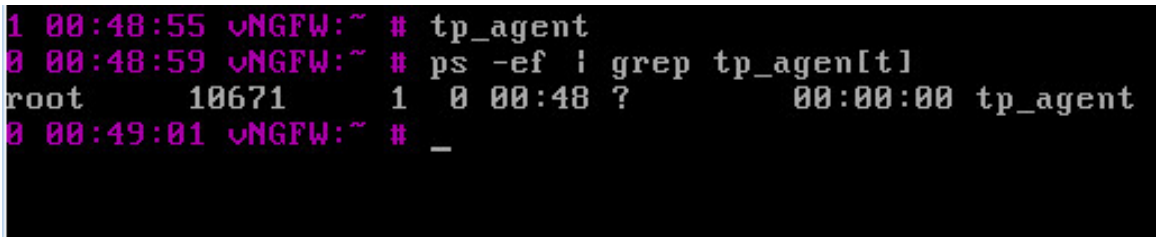
Check status of the SVM, find that this SVM is ‘Offline Offline’:



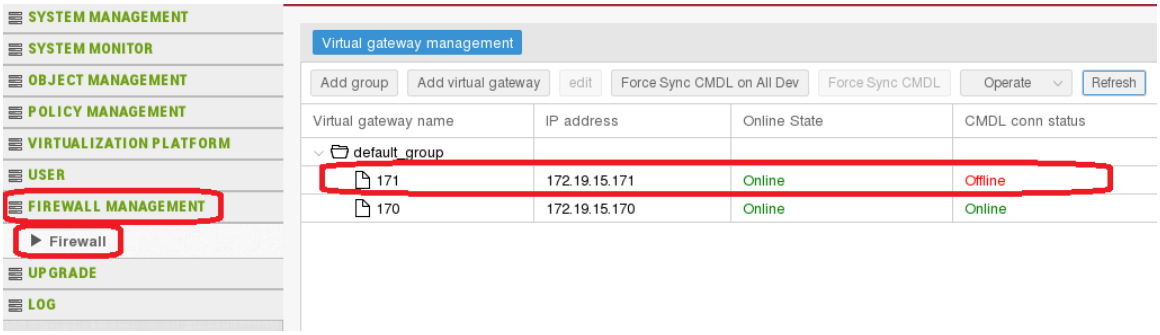
The first ‘Offline’ means that the TCP port 4000 is closed on the SVM. So login to the SVM’s console, look for a process named ‘tp_agent’, but not found:



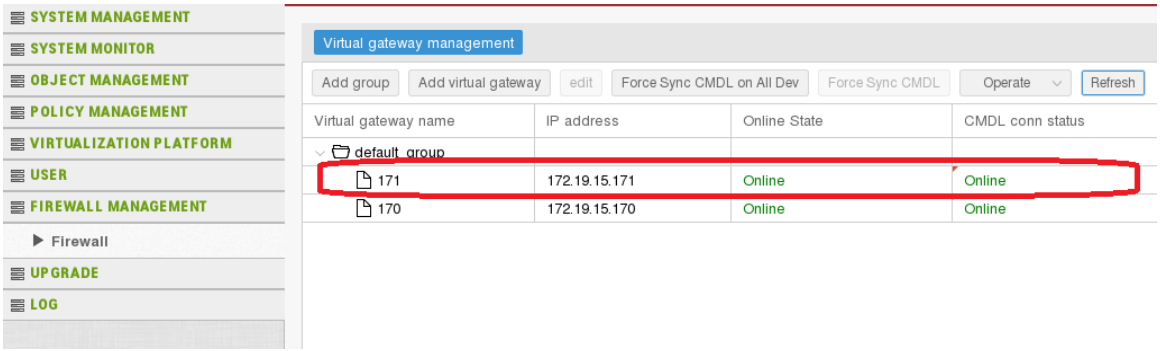
‘tp_agent’ is the process which listens on TCP port 4000, so start it manually



About 20 seconds later, the first status becomes ‘Online’, and the CMDL status is still ‘Offline’:



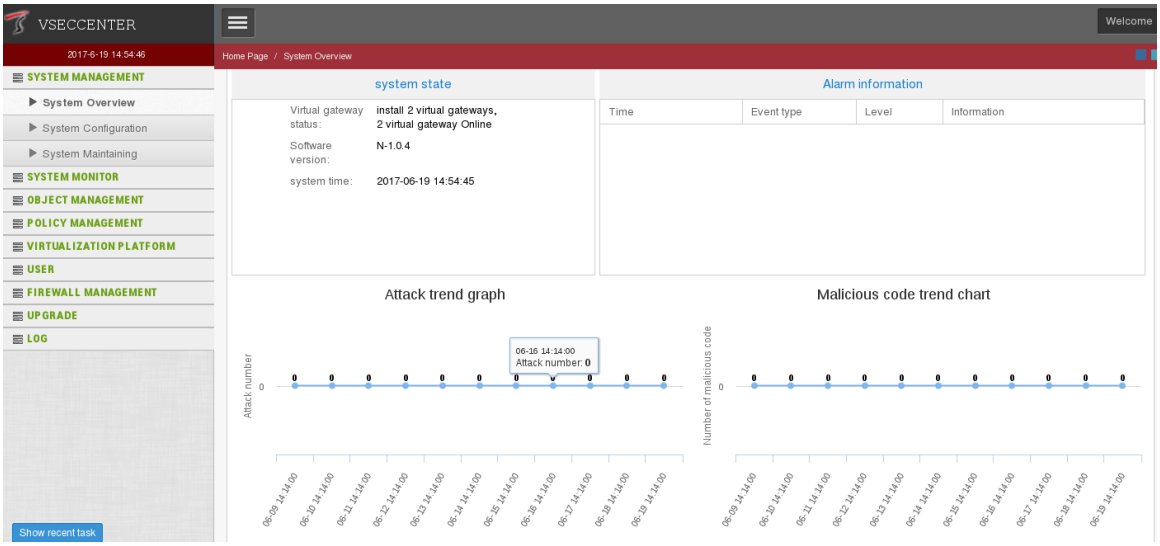
Just wait, or click the ‘Force Sync CMDL’ button above the SVM list. After about 30 seconds, the CMDL status becomes ‘Online’:



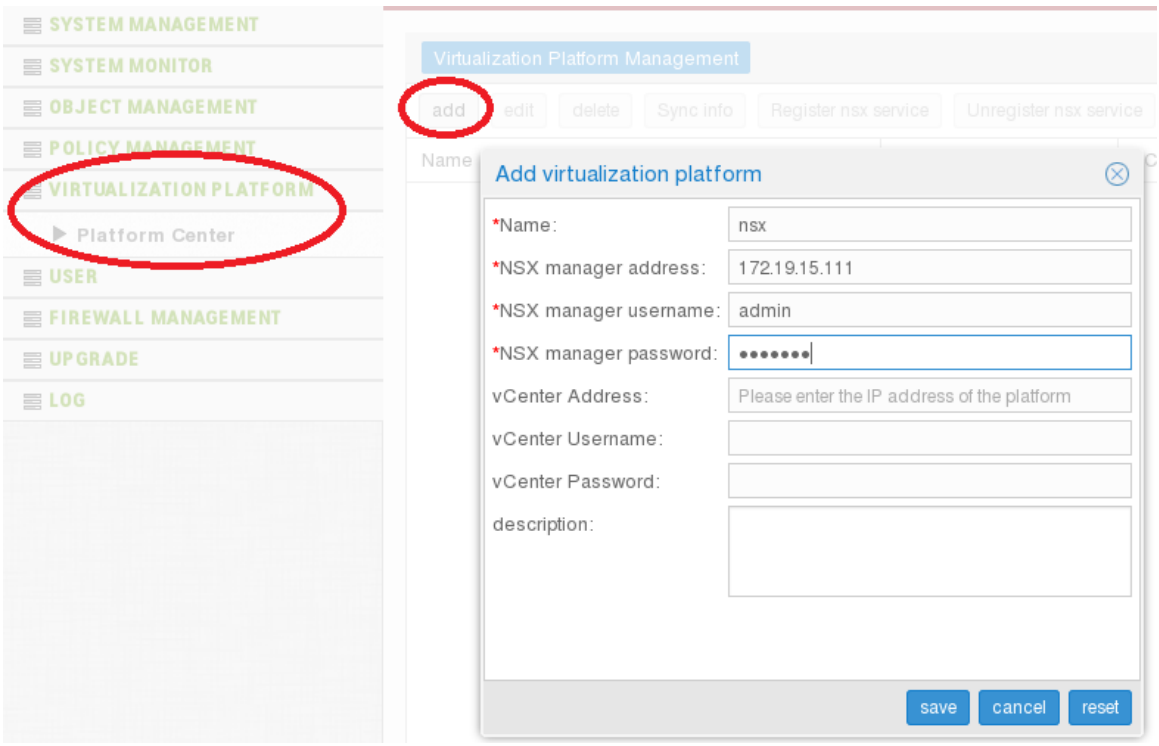
5 Best practices

Demo of the product

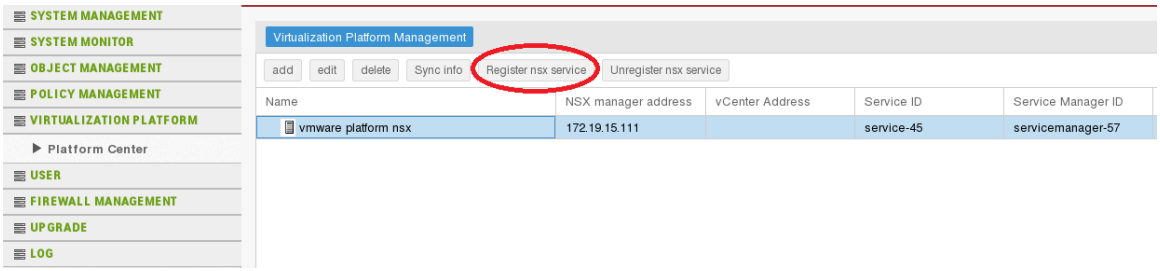
Home Page



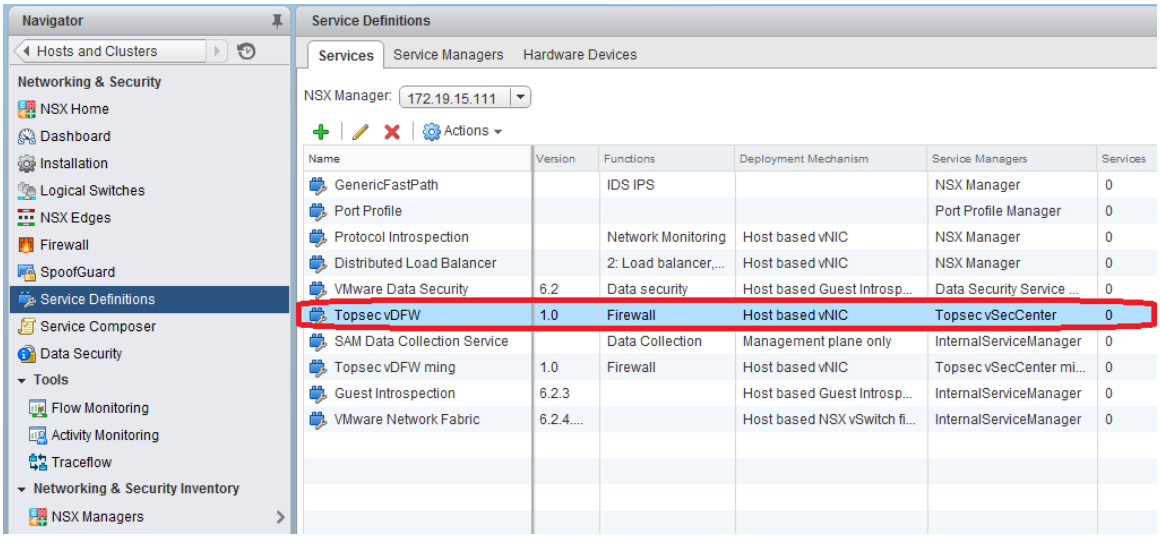
Add NSX Information



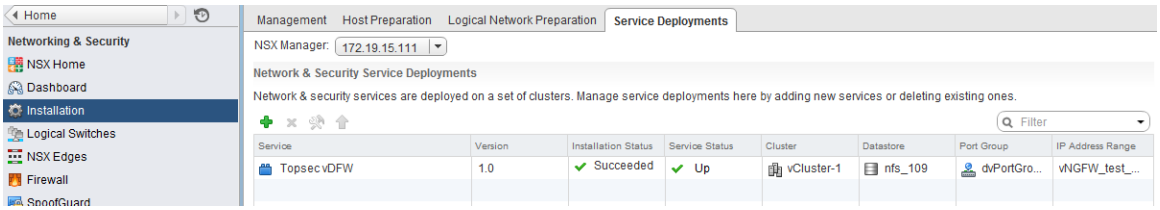
Register Service



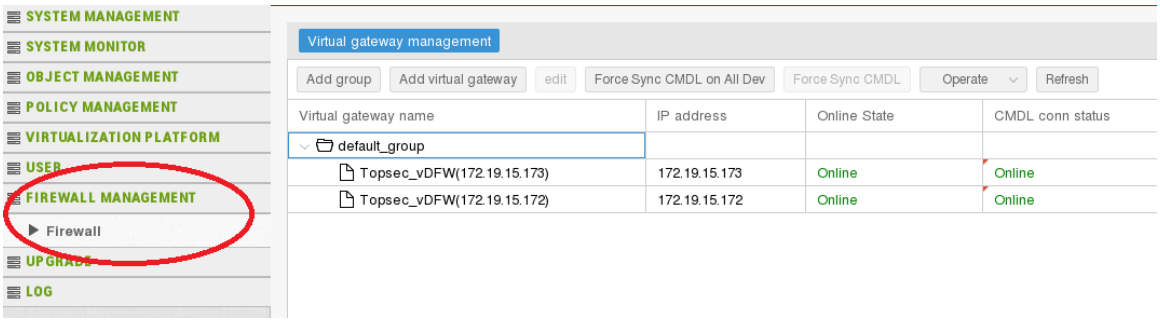
Check Service on NSX



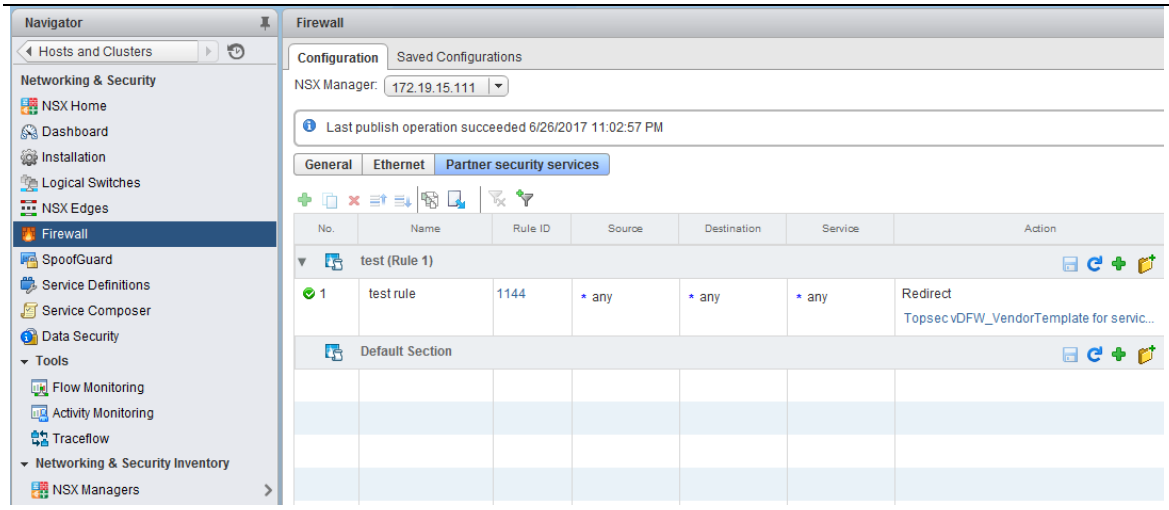
Deploy SVM on NSX UI



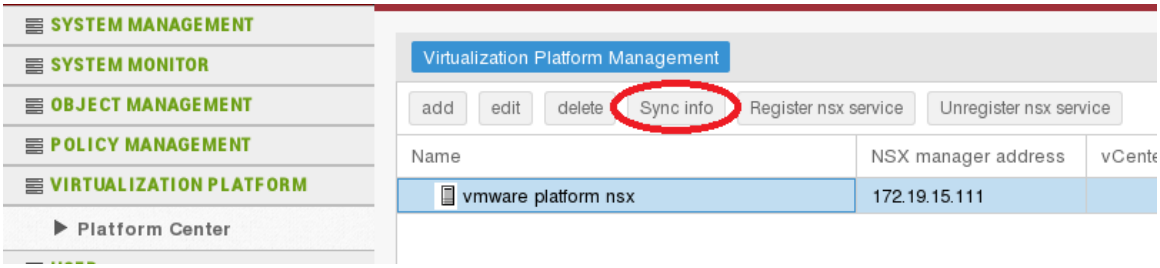
Check Firewall Status



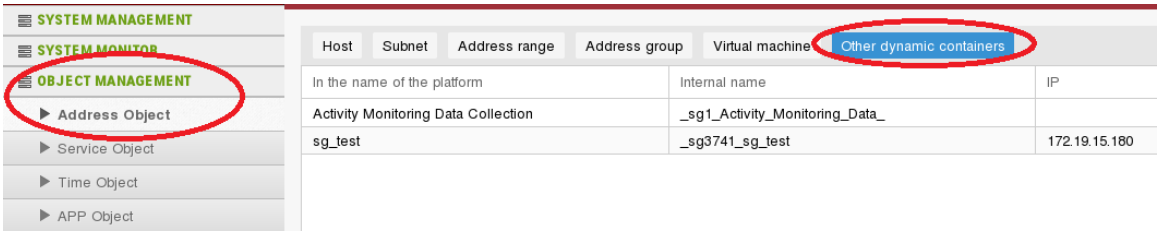
Configure Redirection Policy on NSX UI



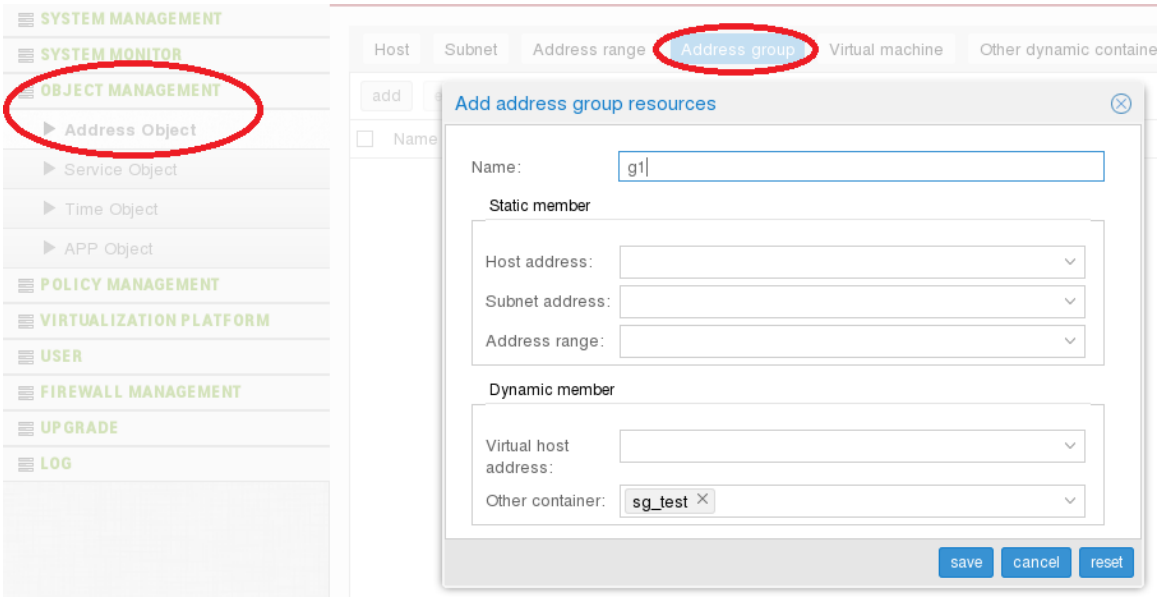
Synchronize Information (Security Groups) from NSX



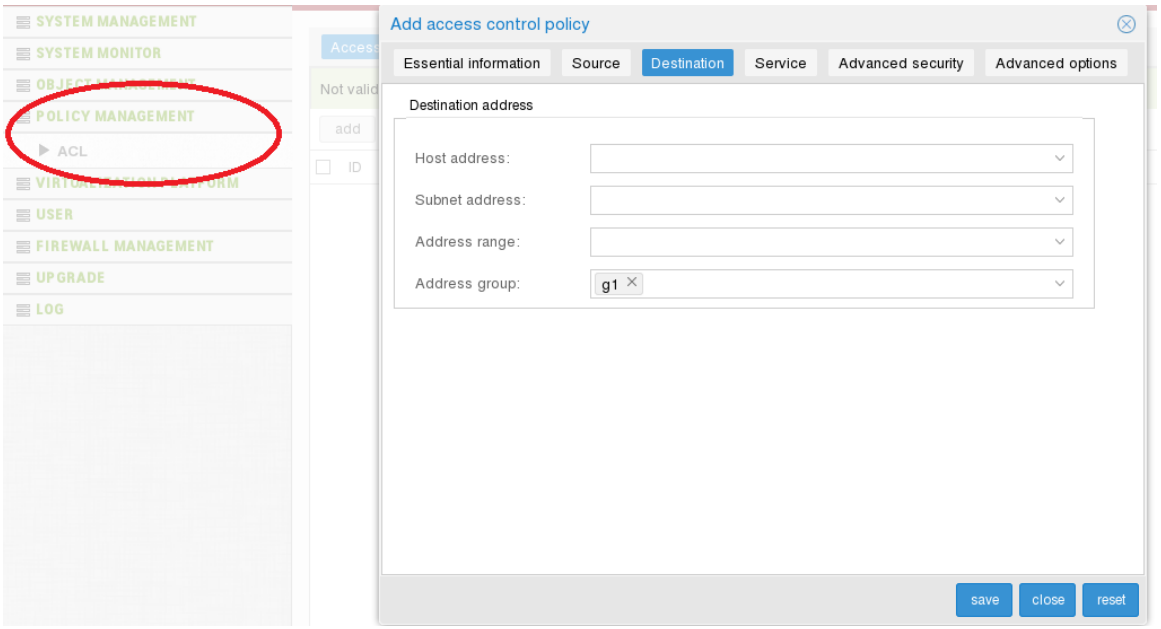
Check Security Groups



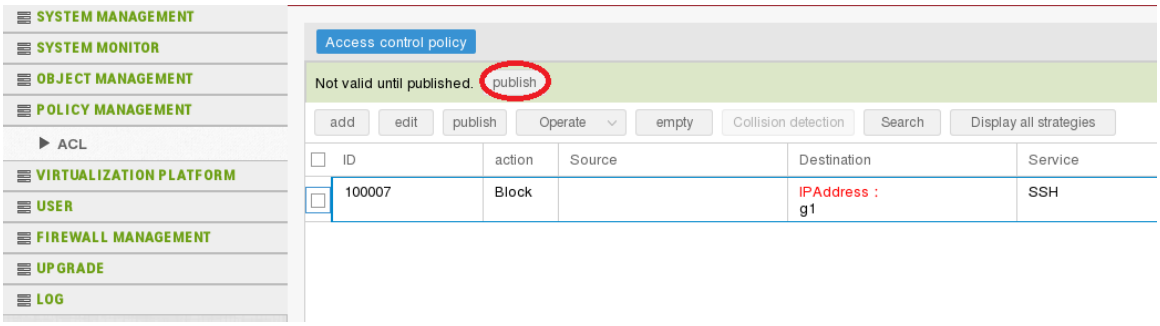
Add Security Group to Address Group



Configure Access Control Policy



Publish to SVMs



Check Firewall Logs