CXS1779BCN

vmware EXPLORE

Demystifying Distributed Security

Tim Burkard (He/Him/His)

Staff Technical Learning Engineer

#vmwareexplore #CXS1779BCN

Required Disclaimer

- This presentation may contain product features or functionality that are currently under development.
- This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

Presenter

Tim Burkard

Staff Technical Learning Engineer

Tim is a VMware employee and has been a technical instructor for 20+ years. He has trained IT professionals in the areas of operating systems, security and networking. Tim specializes in teaching VMware NSX and has previously taught courses covering the entire vSphere product line.

NSX-T Data Center Distributed Protection

You Shall Not Pass!

 Imagery Source: The Lord of the Rings Trilogy, 2001-2003

NSX-T Data Center Distributed Protection

Fly,
you Fools!

 Imagery Source: The Lord of the Rings Trilogy, 2001-2003

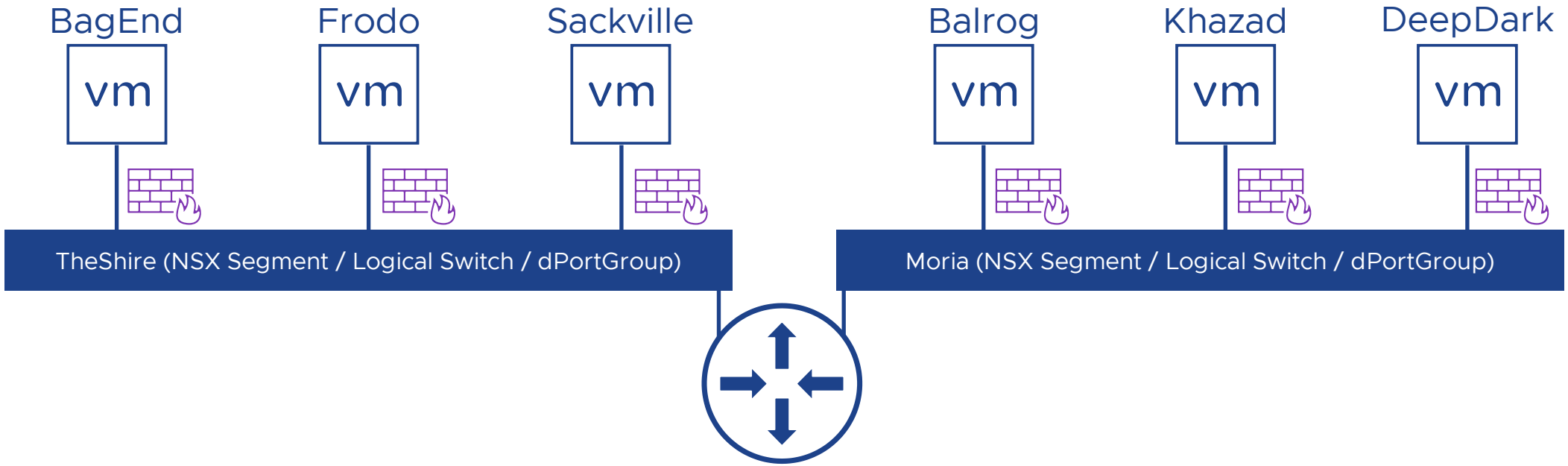
Agenda

1. VMware NSX Distributed Protection
2. NSX Native Tools
3. Using the CLI to Validate DFW Results

VMware NSX Distributed Protection

NSX Distributed Protection

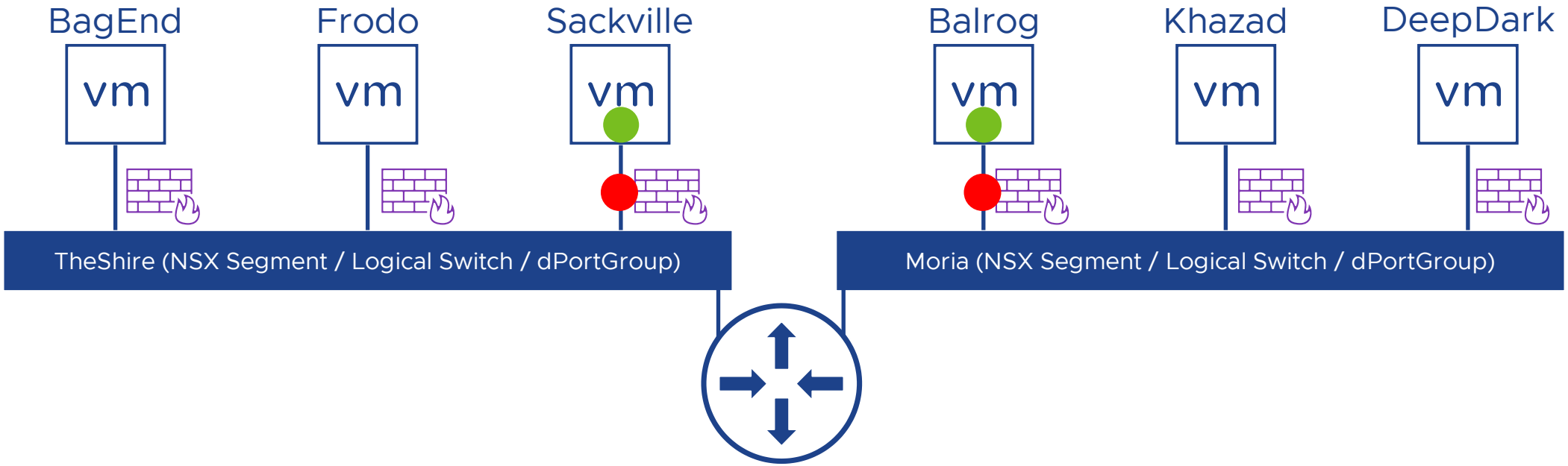
You Shall Not Pass!



Fly, you fools!

NSX Distributed Protection

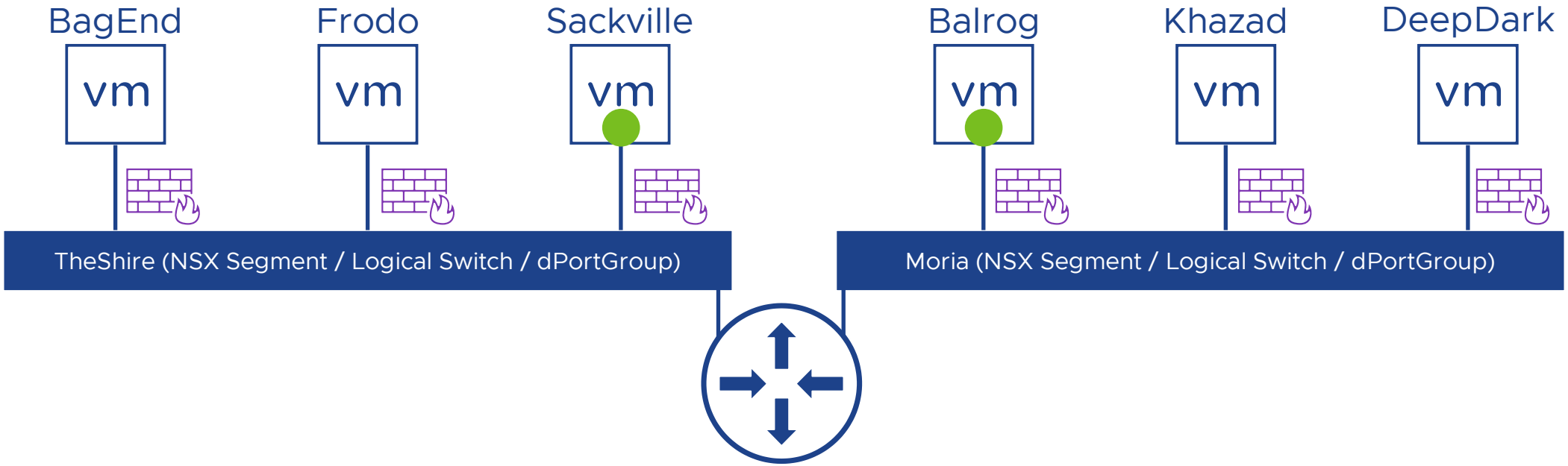
You Shall Not Pass!



Fly, you fools!

NSX Distributed Protection

You Shall Not Pass!



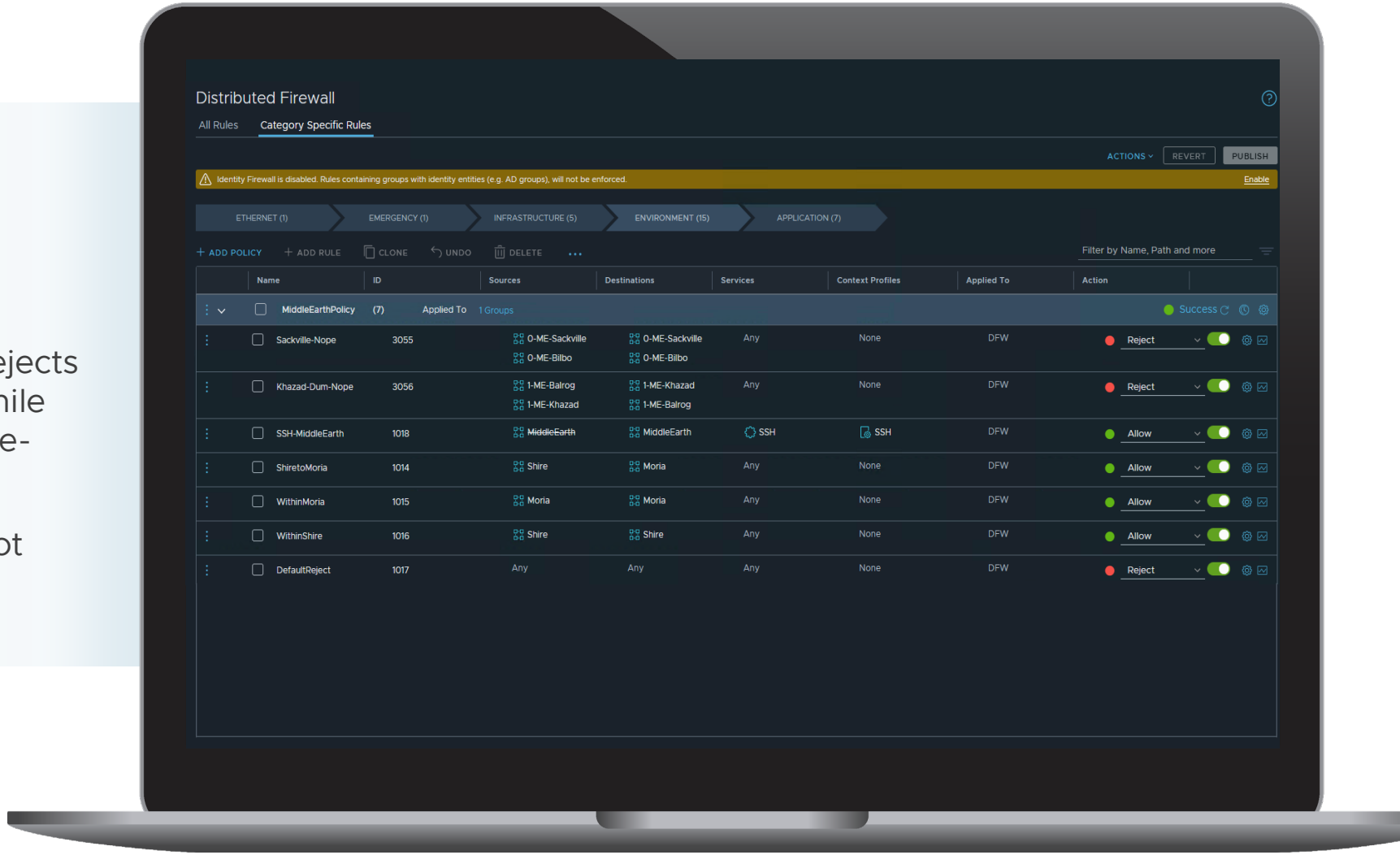
Fly, you fools!

NSX Distributed Protection

Distributed Firewall (DFW) Policy contains rules

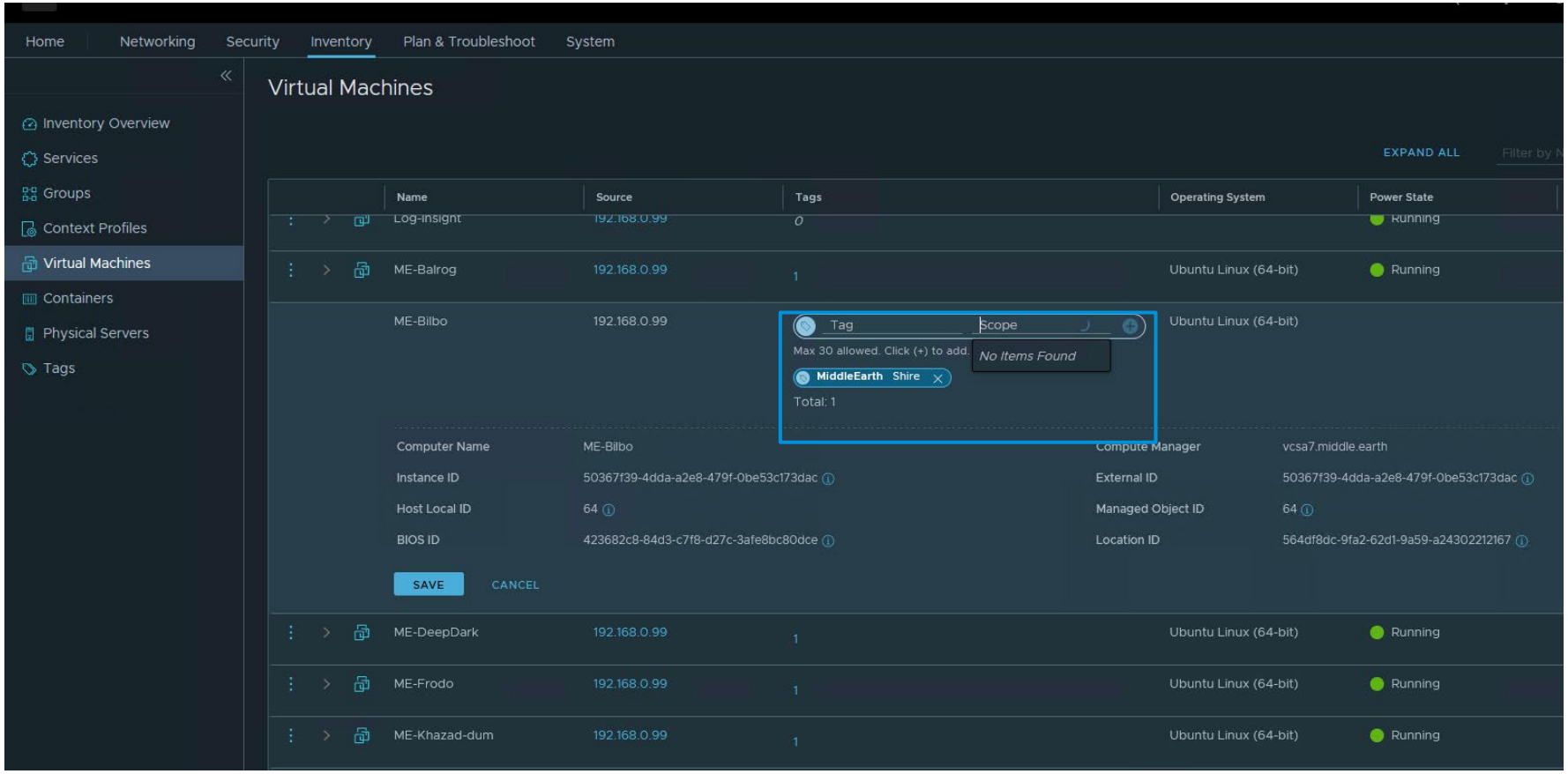
The Rules in the MiddleEarthPolicy rejects specific VM to VM communication while allowing intra-segment traffic and one-way traffic from Shire to Moria.

The Policy Default rejects anything not allowed leading to Zero Trust



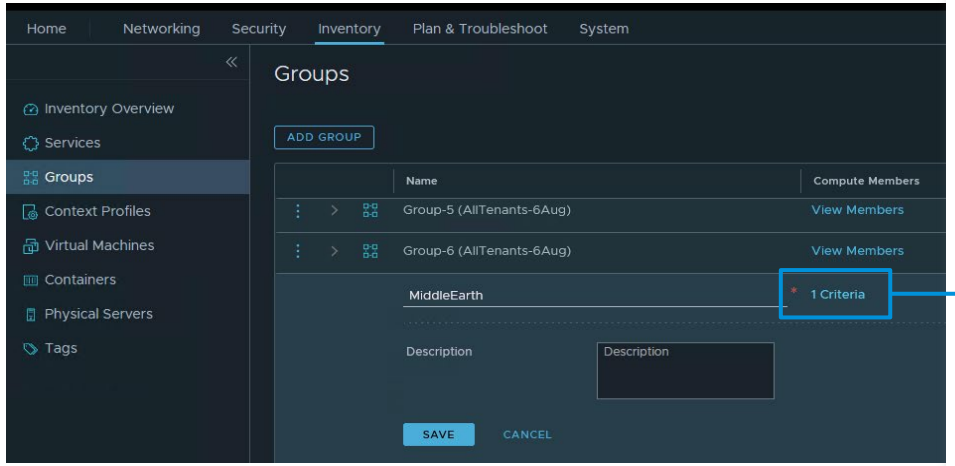
NSX Distributed Protection

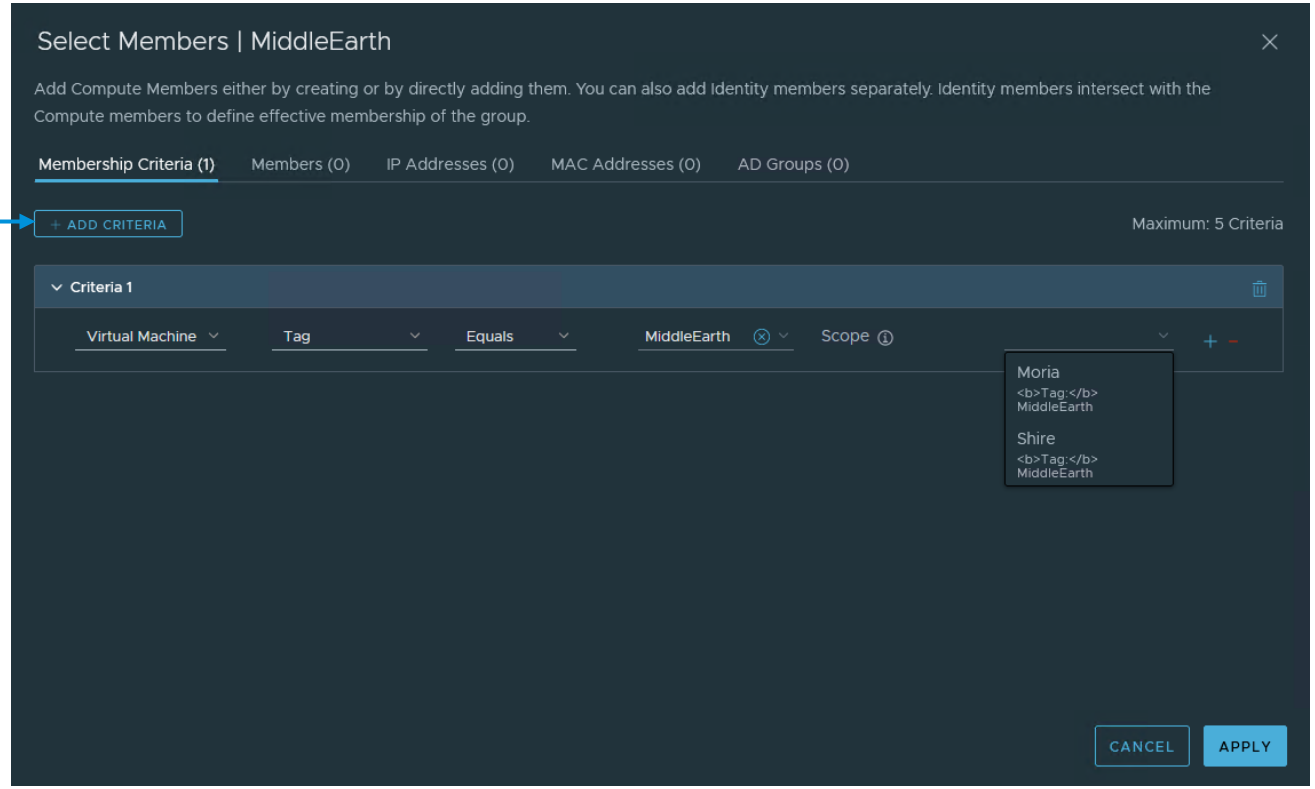
Tagging Virtual Machines as an attribute of the VM



NSX Distributed Protection

Put a Group Together using the Tags

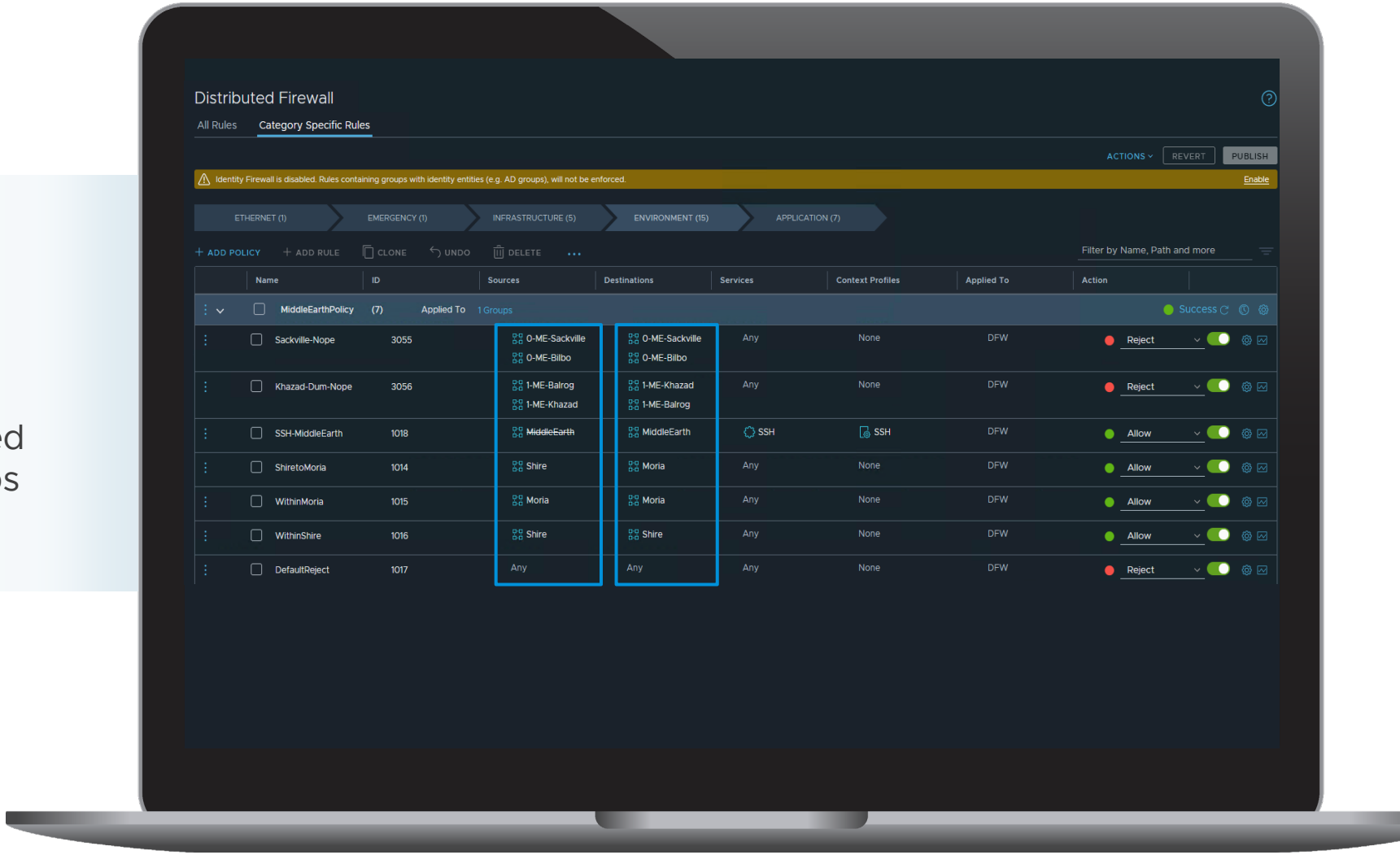




NSX Distributed Protection

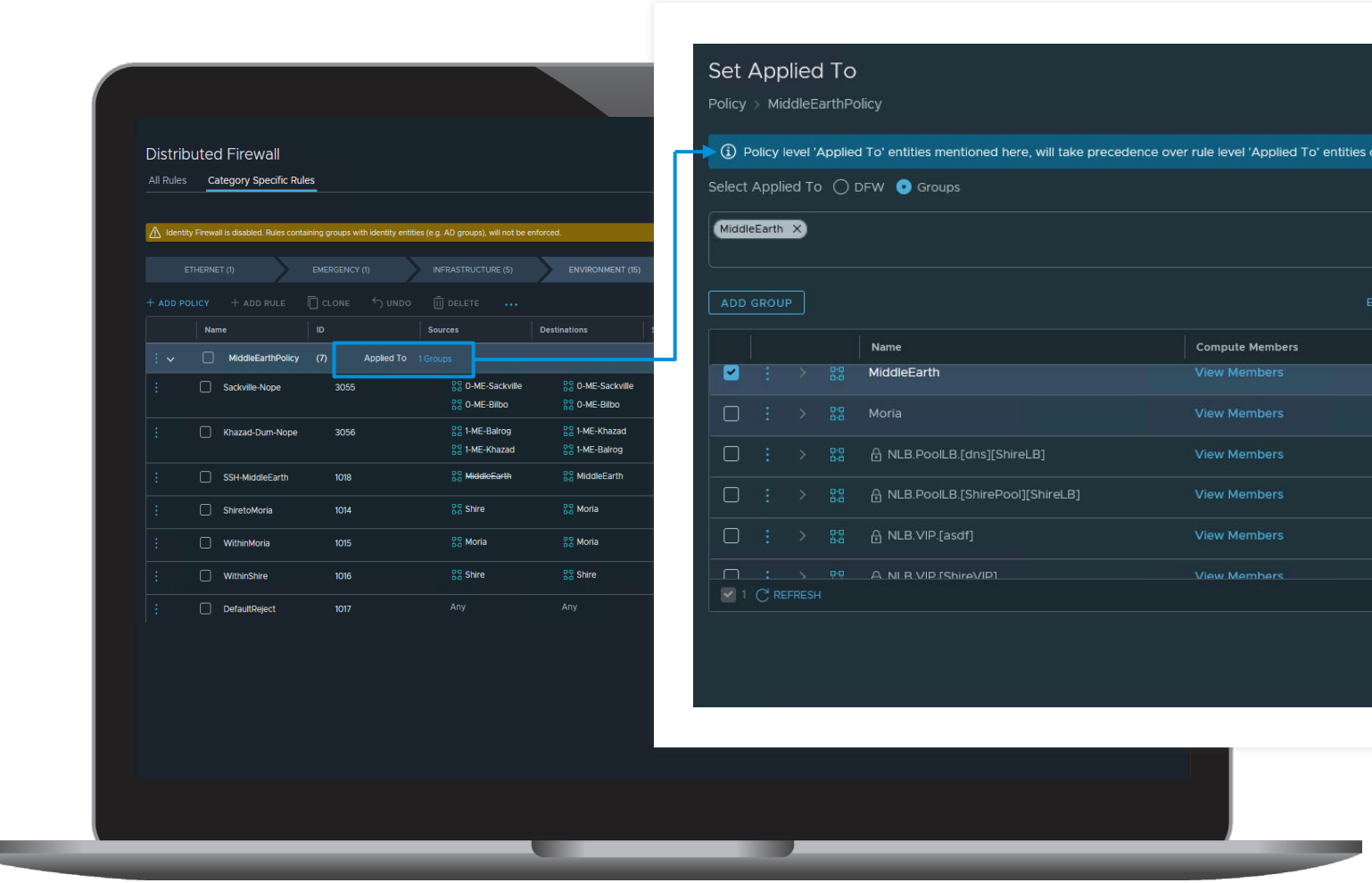
Groups make life easier to populate DFW fields in each rule

Source, Destination and the Applied to Fields were populated by Groups built on Security Tags



NSX Distributed Protection

Two options for Applied to: Policy and each rule. Policy has priority.

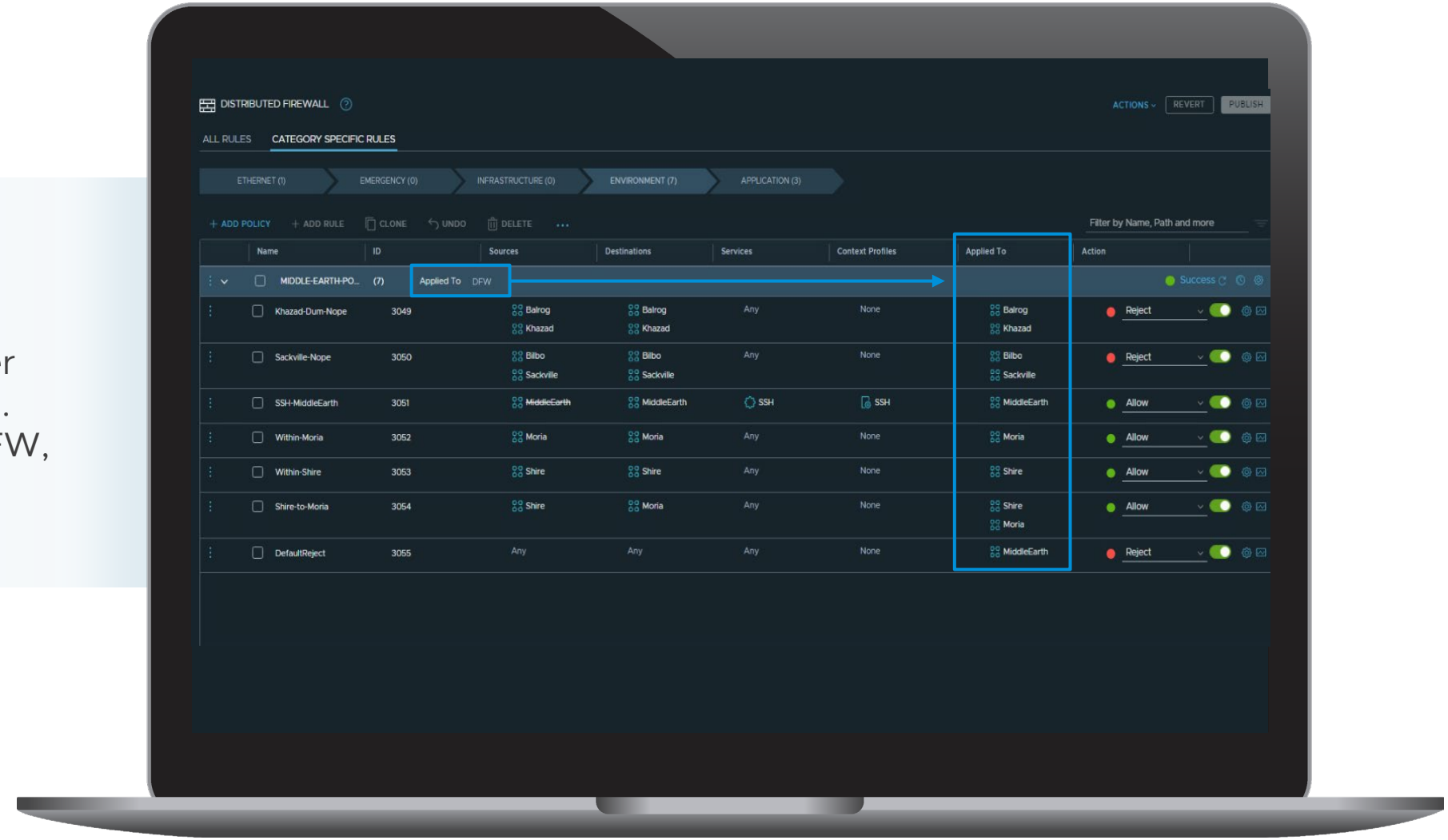


When using the Applied To field for the Policy, the Rule Applied To is prioritized over the Applied To for each rule.

NSX Distributed Protection

Two options for Applied to: Policy and each rule. Policy has priority.

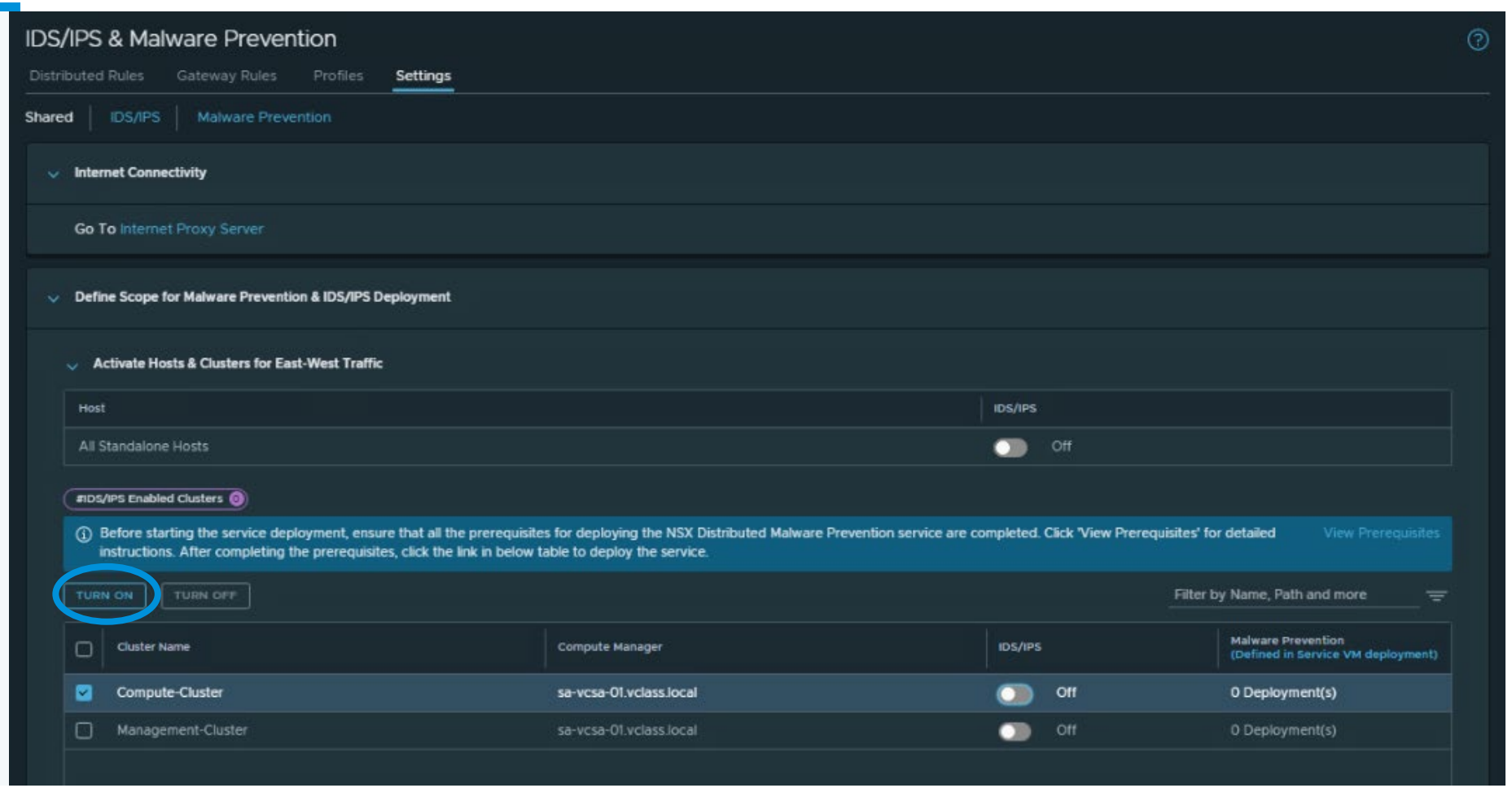
When using the Applied To field for the Policy, the Rule Applied To is prioritized over the Applied To for each rule. But if Policy is applied to DFW, Rule can be very granular.



NSX Distributed Protection

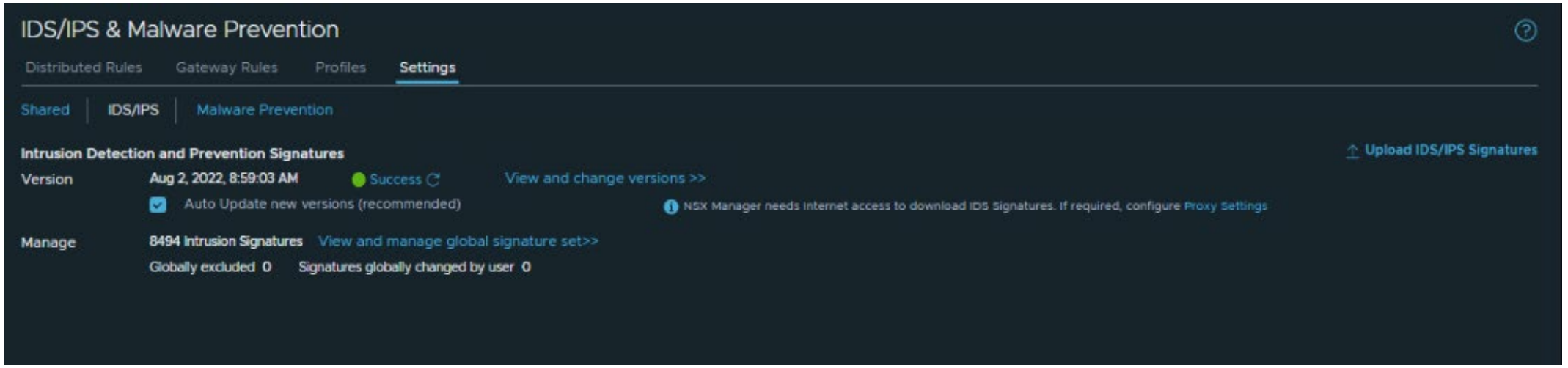
Let’s examine Distributed Intrusion Detection and Prevention

Intrusion Detection and Prevention are enabled in the Settings – Shared Tabs by Individual Cluster or All Standalone Hosts



NSX Distributed Protection

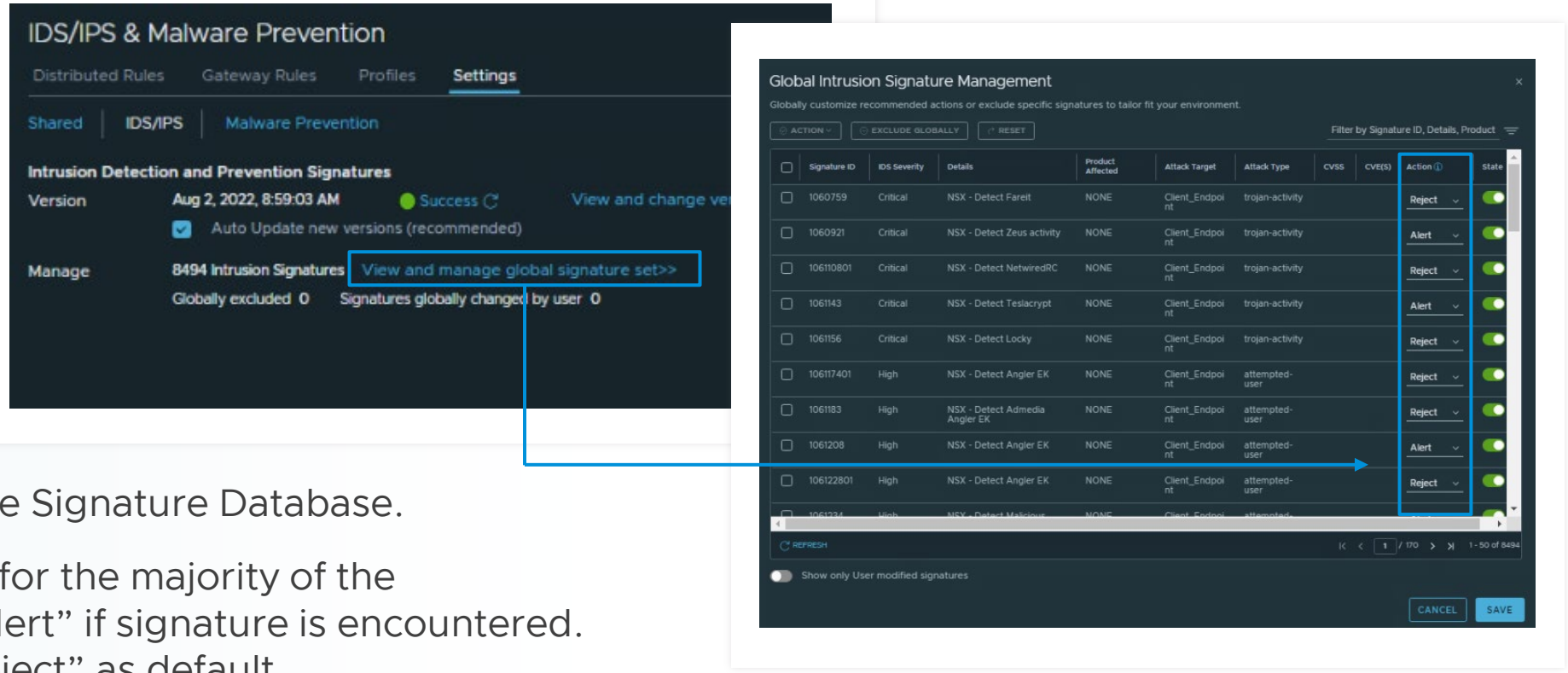
Distributed Intrusion Detection and Prevention Signatures



We then look at the Signature Database.

NSX Distributed Protection

Distributed Intrusion Detection and Prevention Signatures



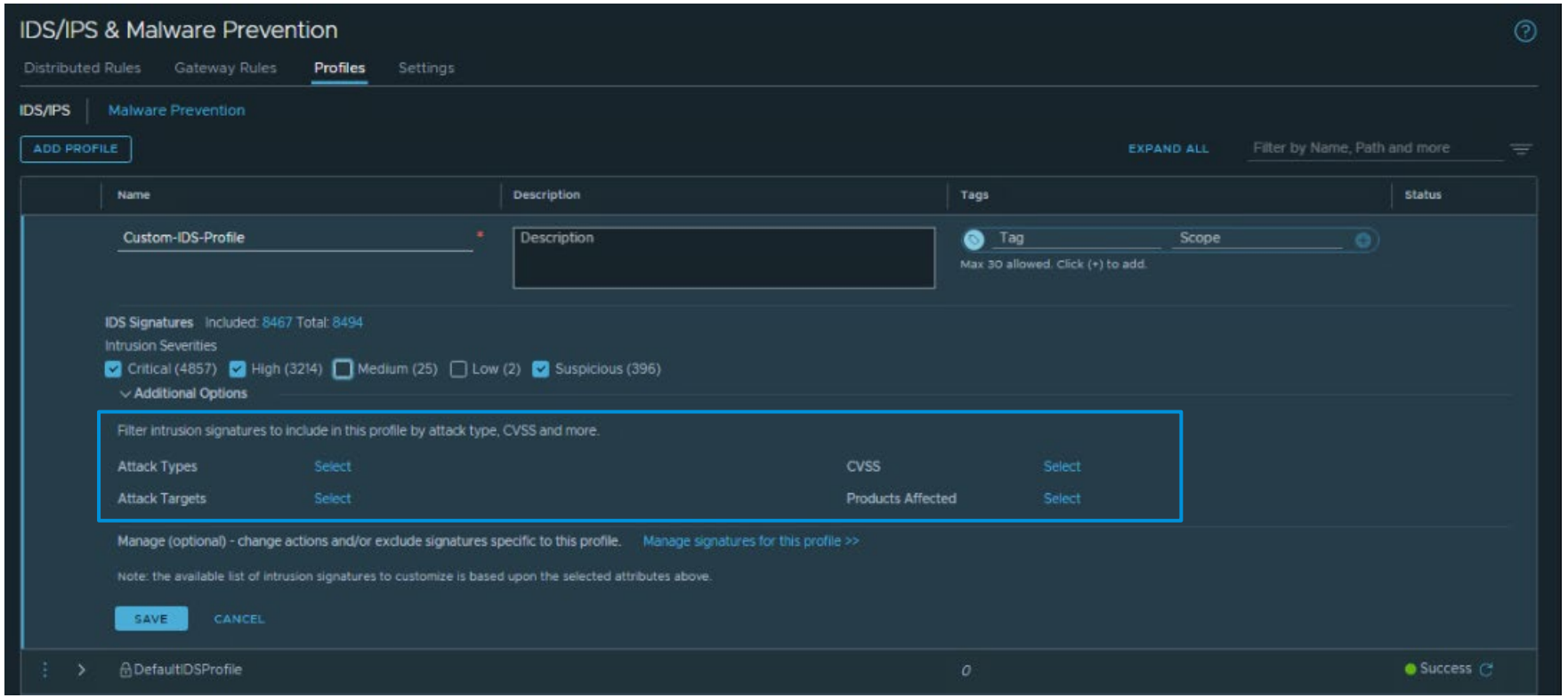
We then look at the Signature Database.

The default action for the majority of the signatures is to “Alert” if signature is encountered. A minority has “Reject” as default.

This fact becomes important in Intrusion Prevention.

NSX Distributed Protection

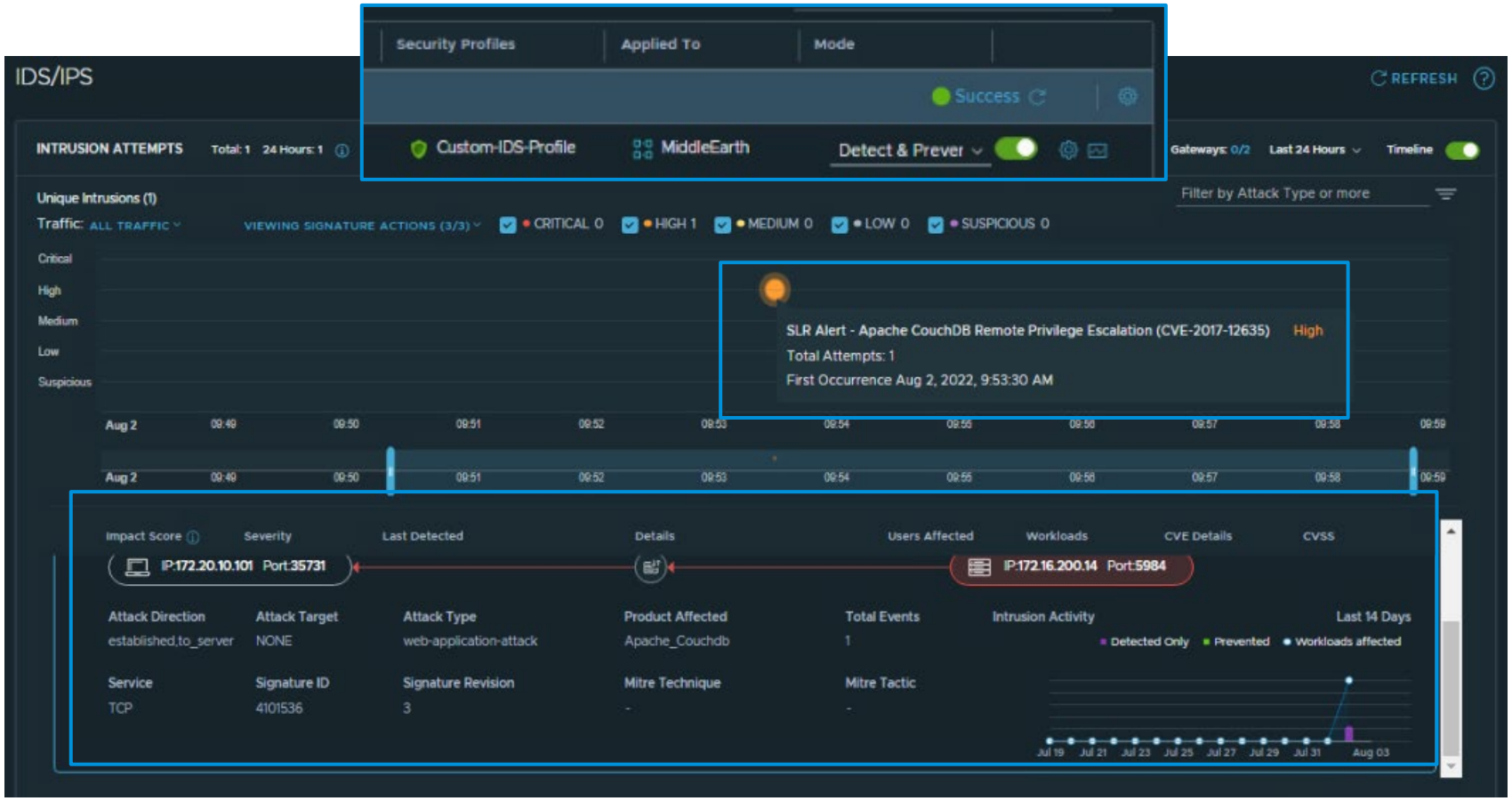
Distributed Intrusion Detection and Prevention Profiles



Profiles are the description of the IDS Signatures to be examined, by severity and inclusion based on Types, Targets, CVSS or Products.

NSX Distributed Protection

Distributed Intrusion Detection and Prevention Setup for Prevention (Drop or Reject)

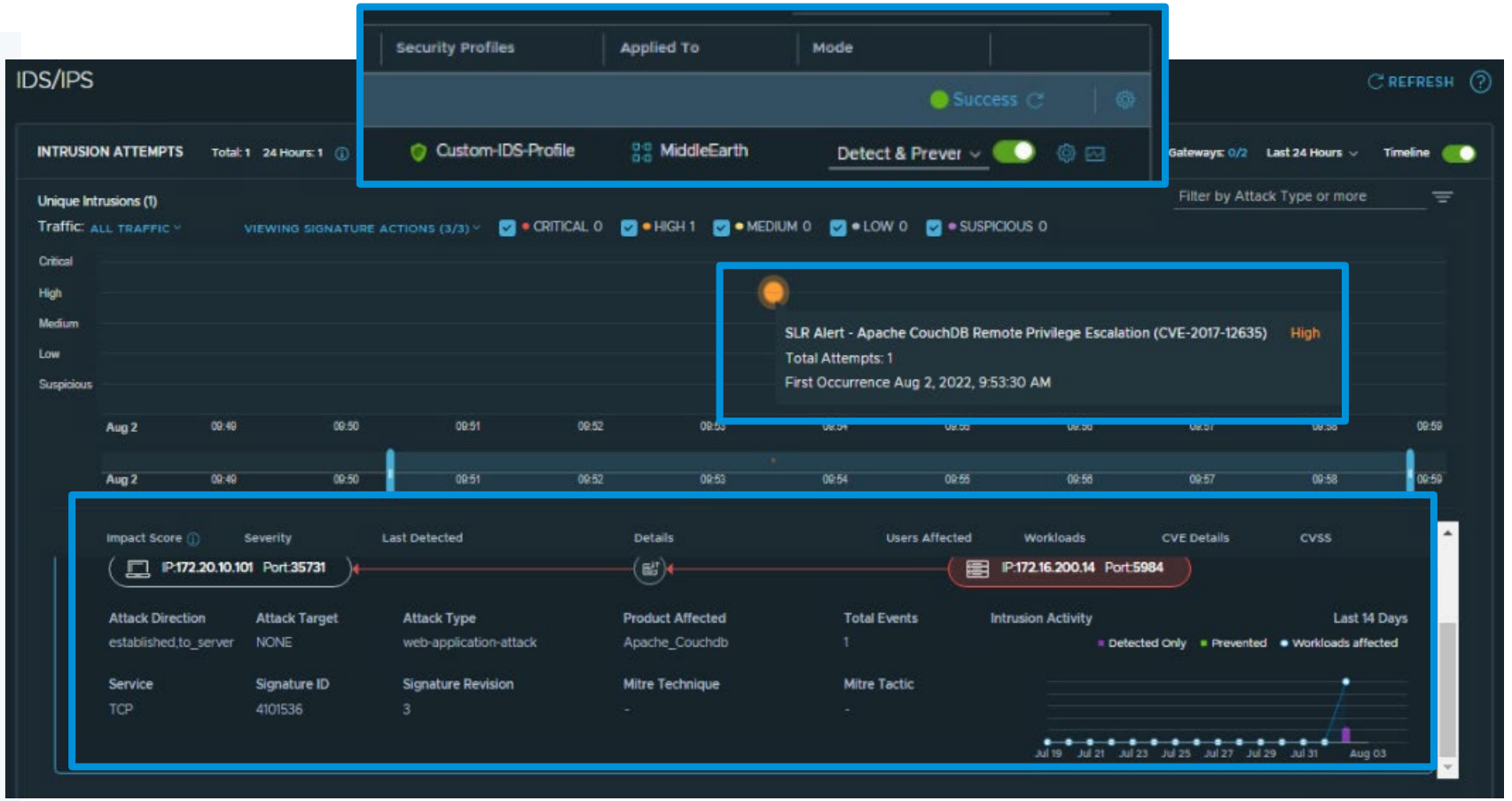


If the rule is modified to **Detect and Prevent**…

NSX Distributed Protection

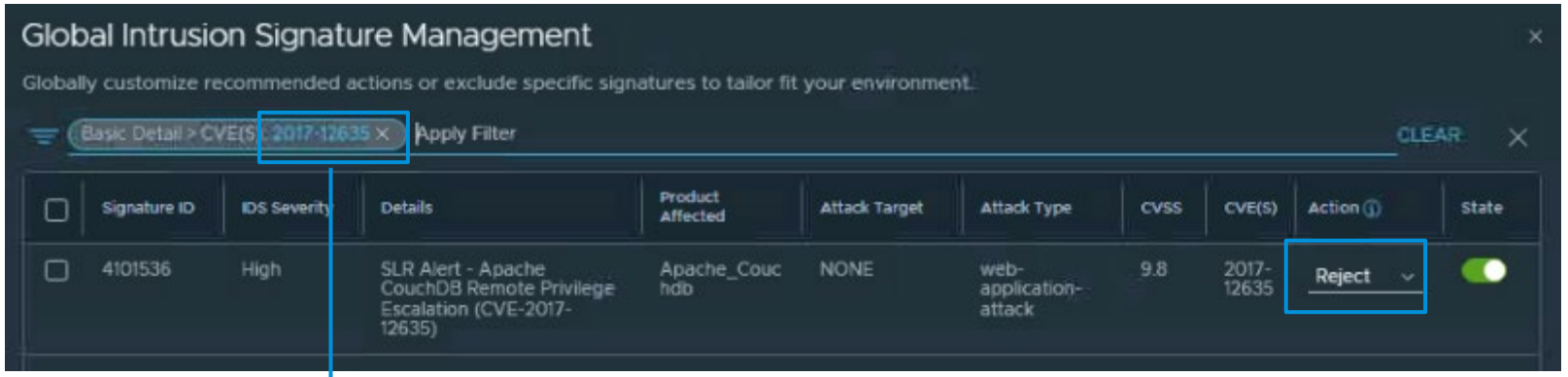
Distributed Intrusion Detection and Prevention Setup for Prevention (Drop or Reject)

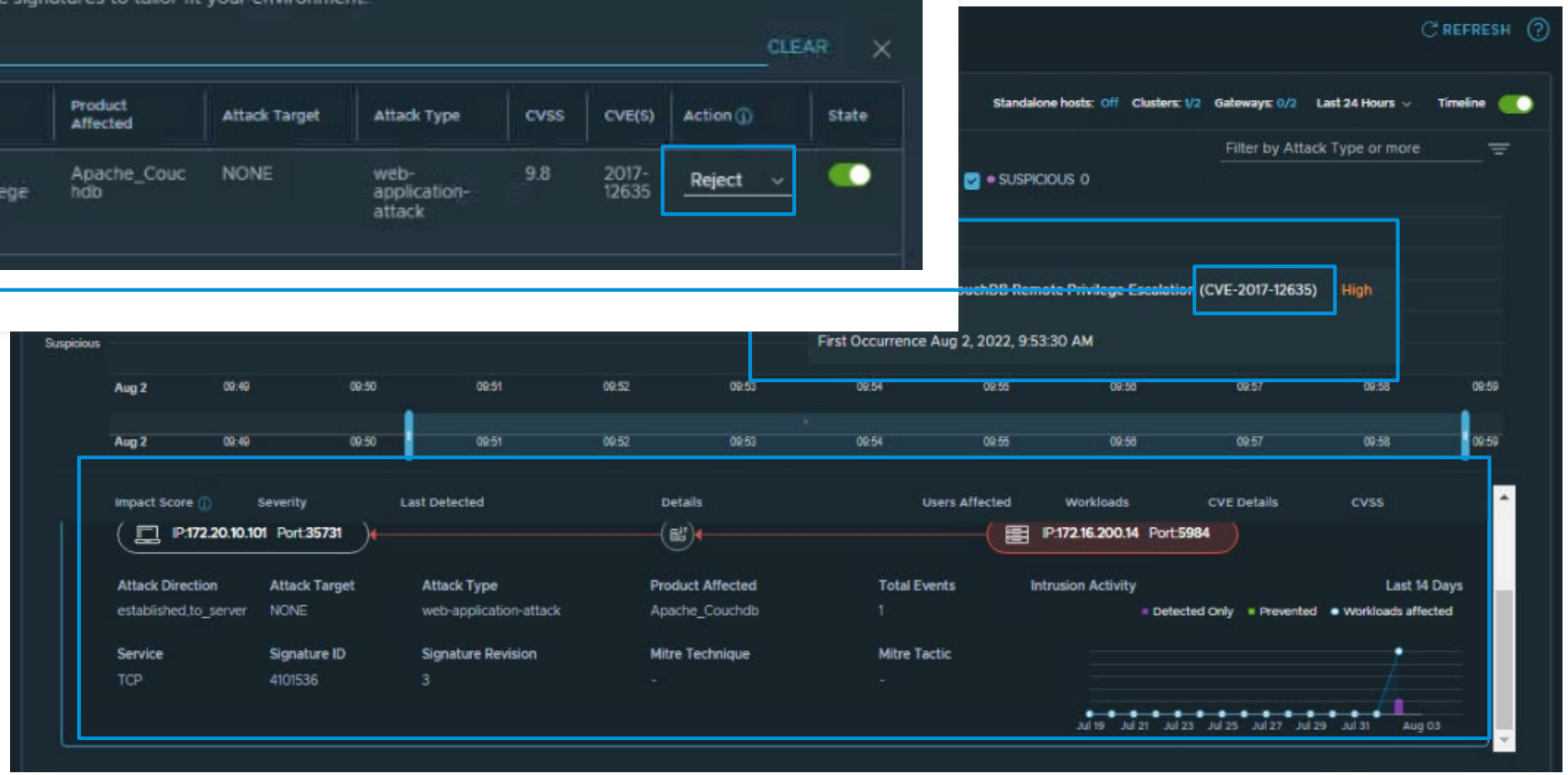
If the rule is modified to Detect and Prevent…



NSX Distributed Protection

Distributed Intrusion Detection and Prevention Setup for Prevention (Drop or Reject)



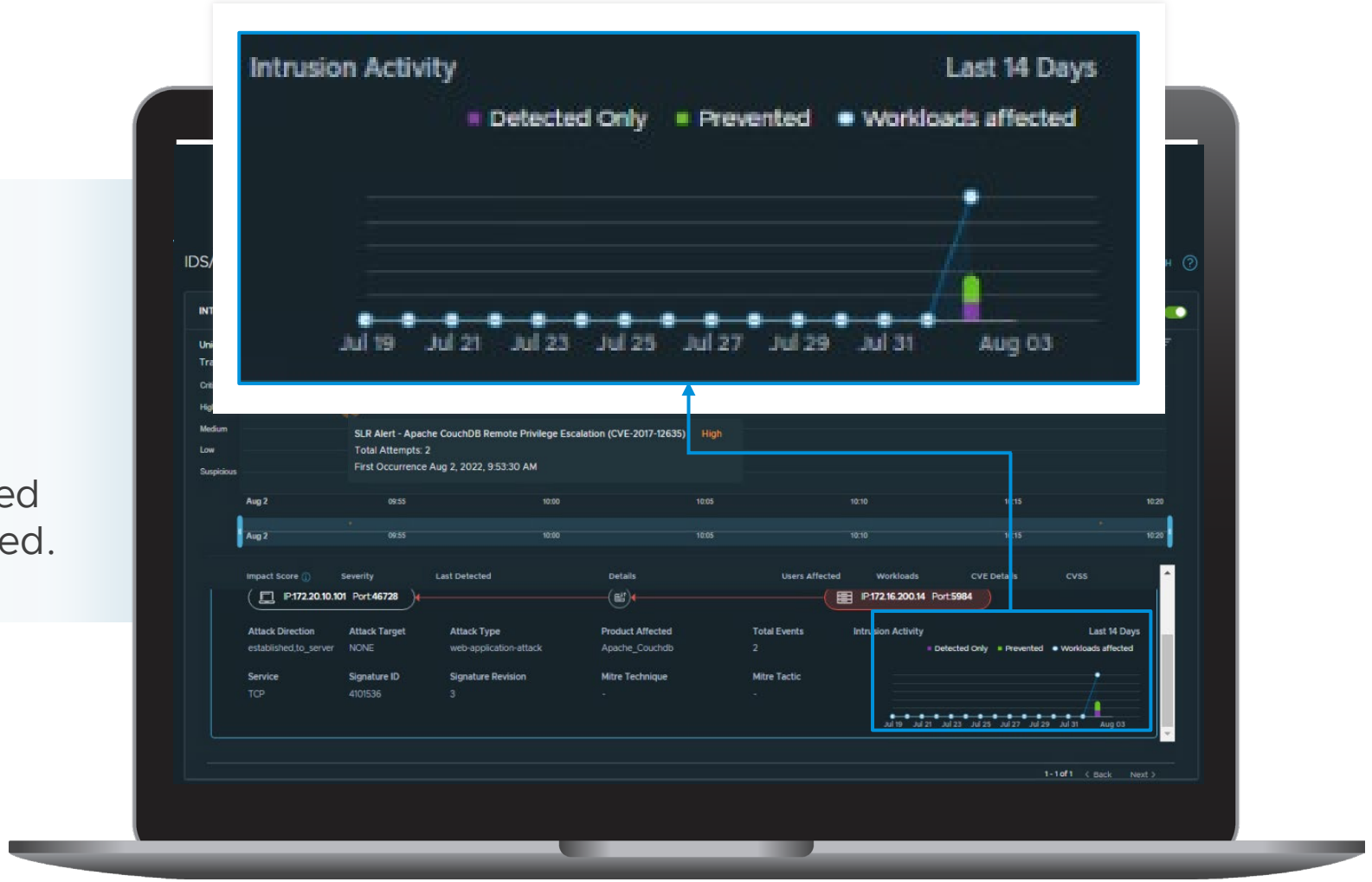


If the rule is modified to Detect and Prevent… the Signature must have an action of Drop or Reject to effectively prevent this flow.

NSX Distributed Protection

Distributed Intrusion Detection and Prevention Results

IPS results show in the same interface with a green bar added to the chart indicating Prevented.



NSX Native Tools

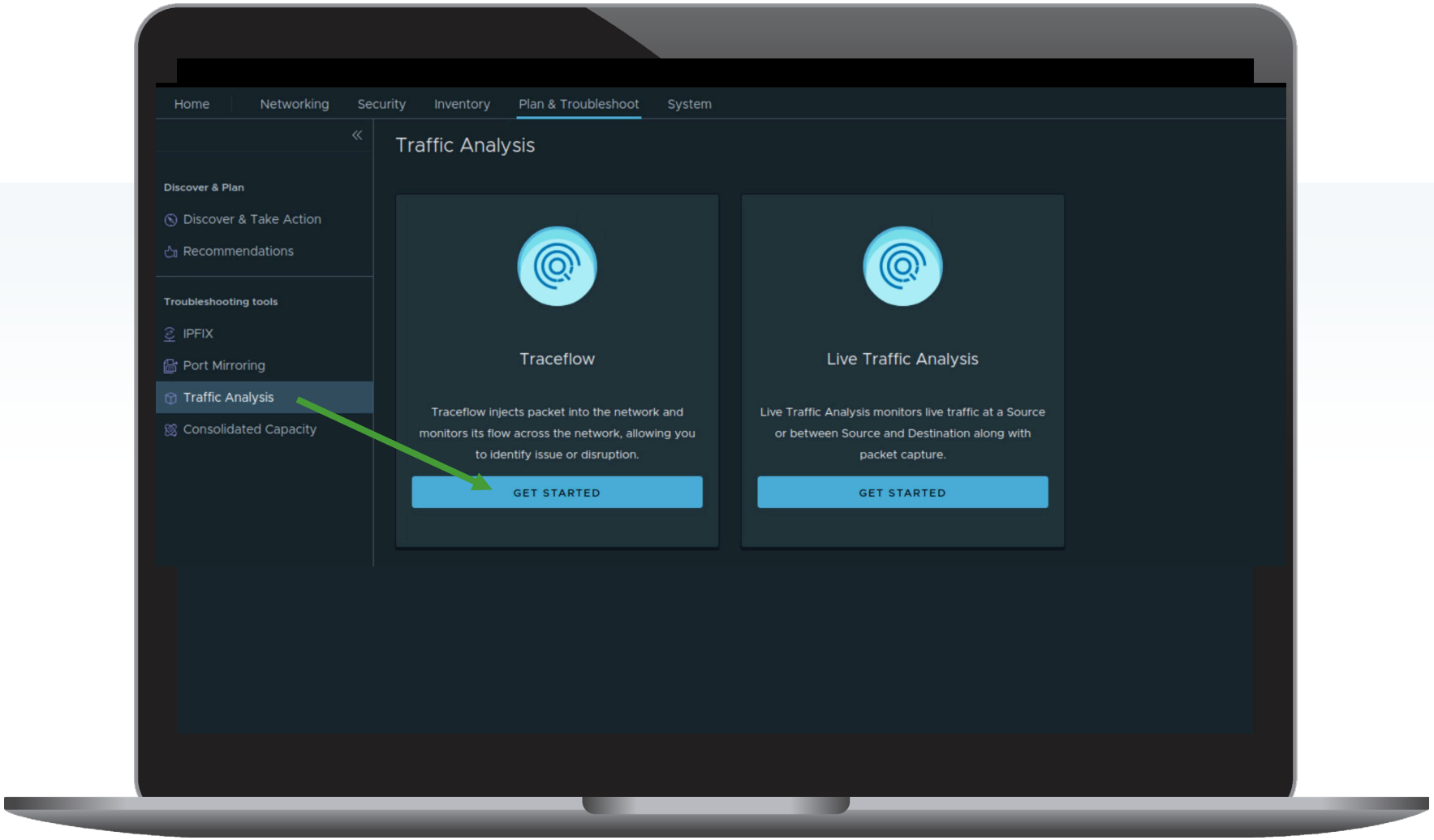
Tools used for troubleshooting the NSX-T Data Center Distributed Firewall (DFW):

Traffic Analysis

- Traceflow
- Live Traffic Analysis

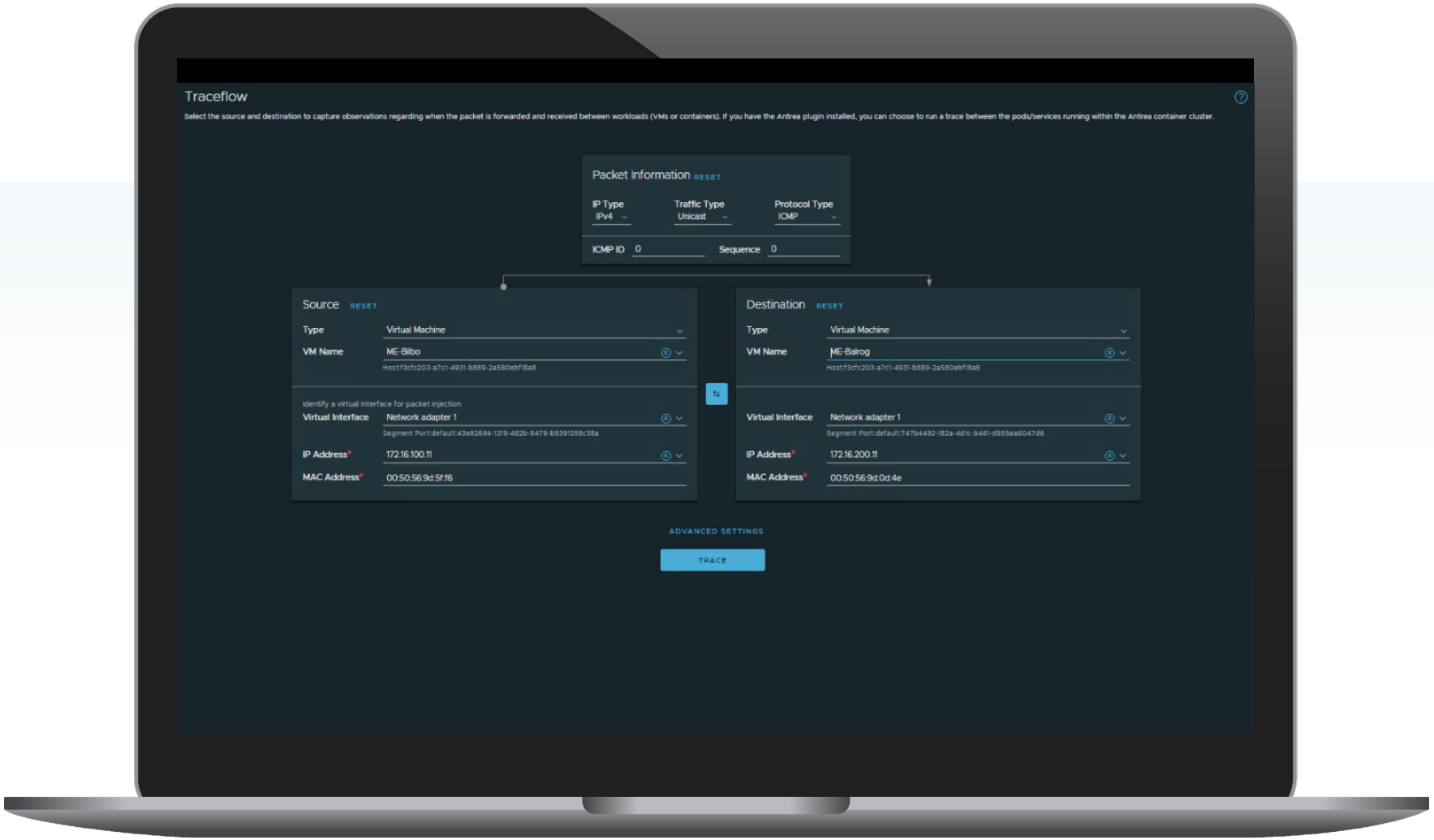
NSX Built in Tools

Traceflow



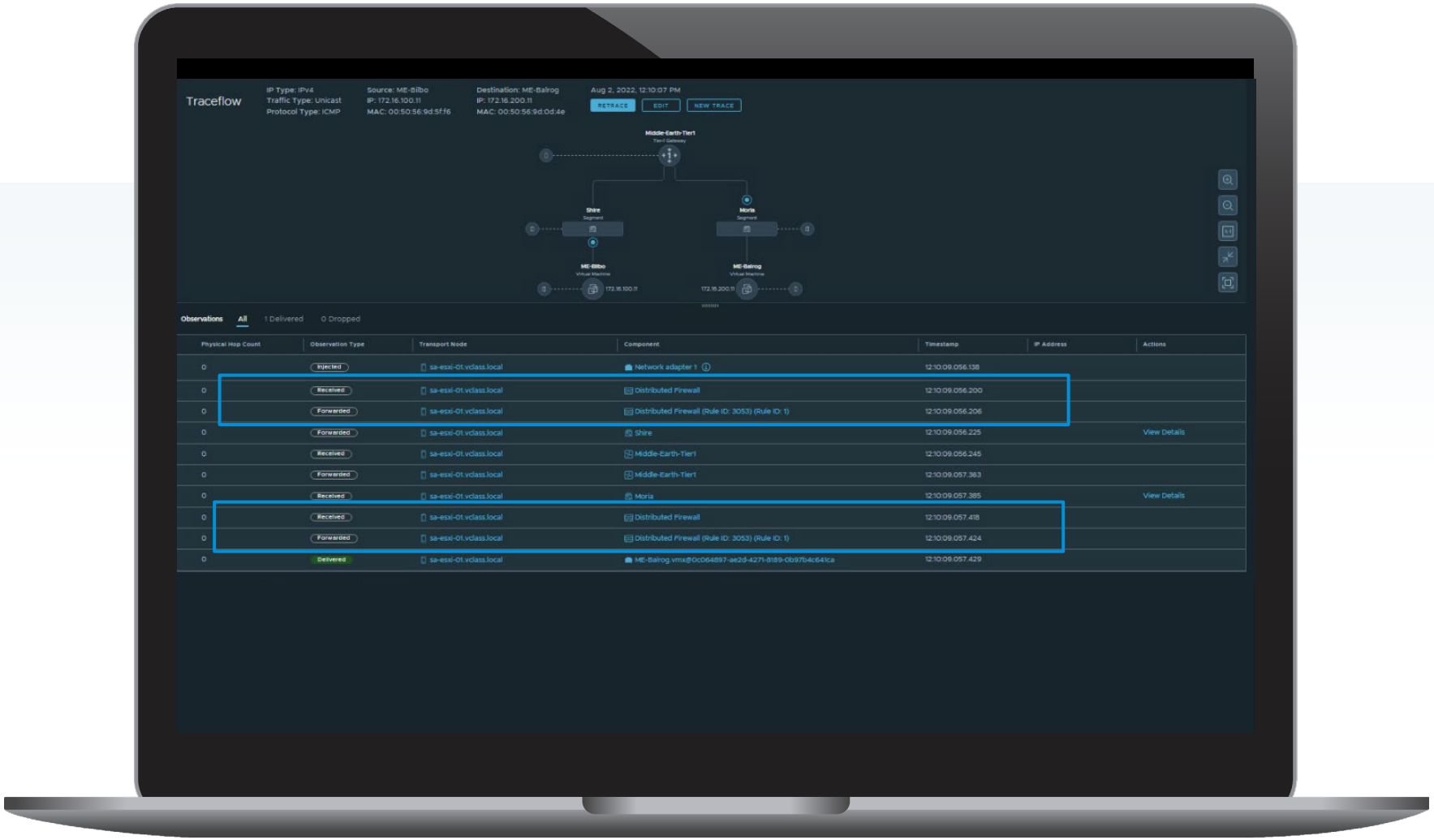
NSX Built in Tools

Traceflow



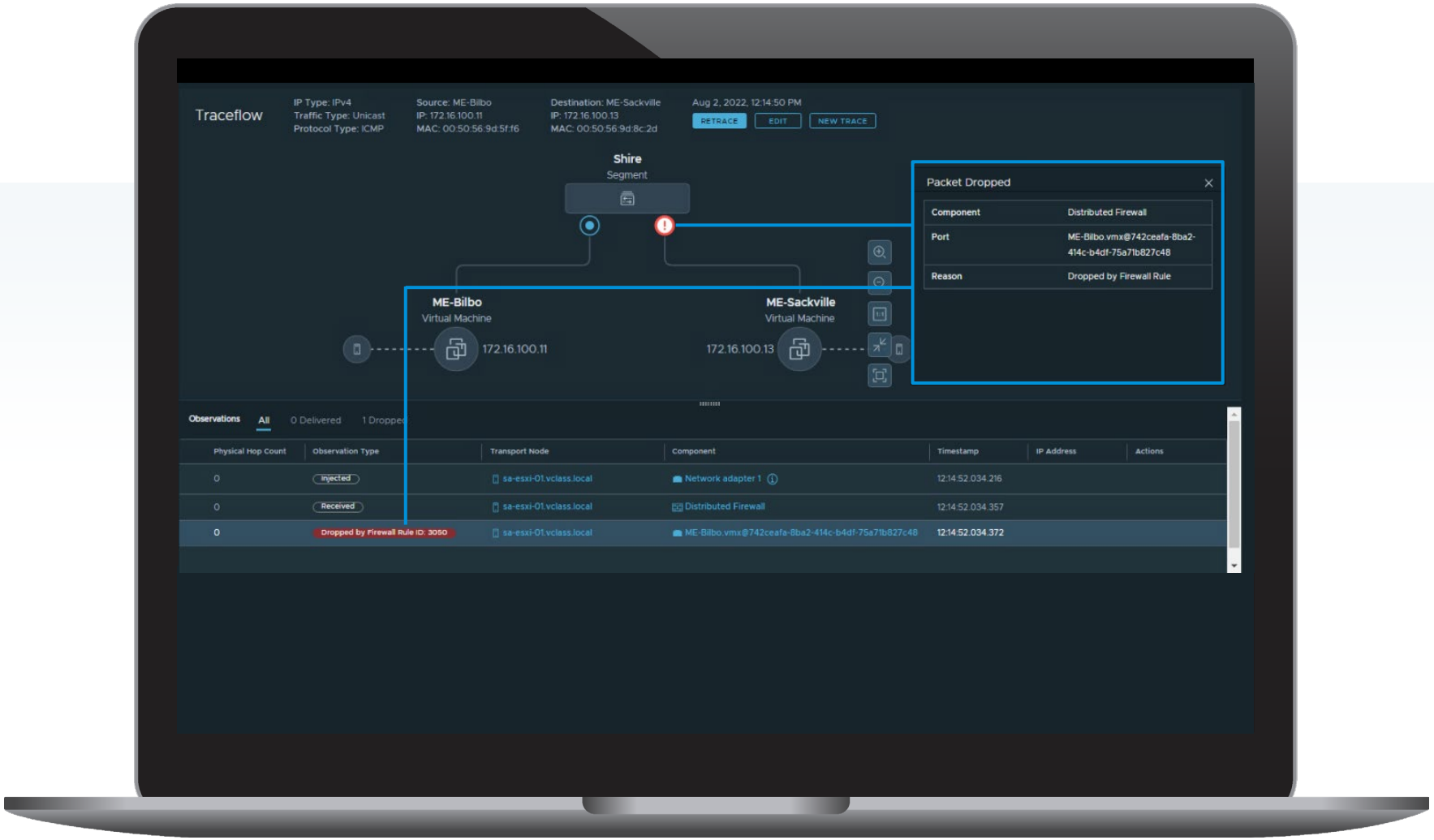
NSX Built in Tools

Traceflow



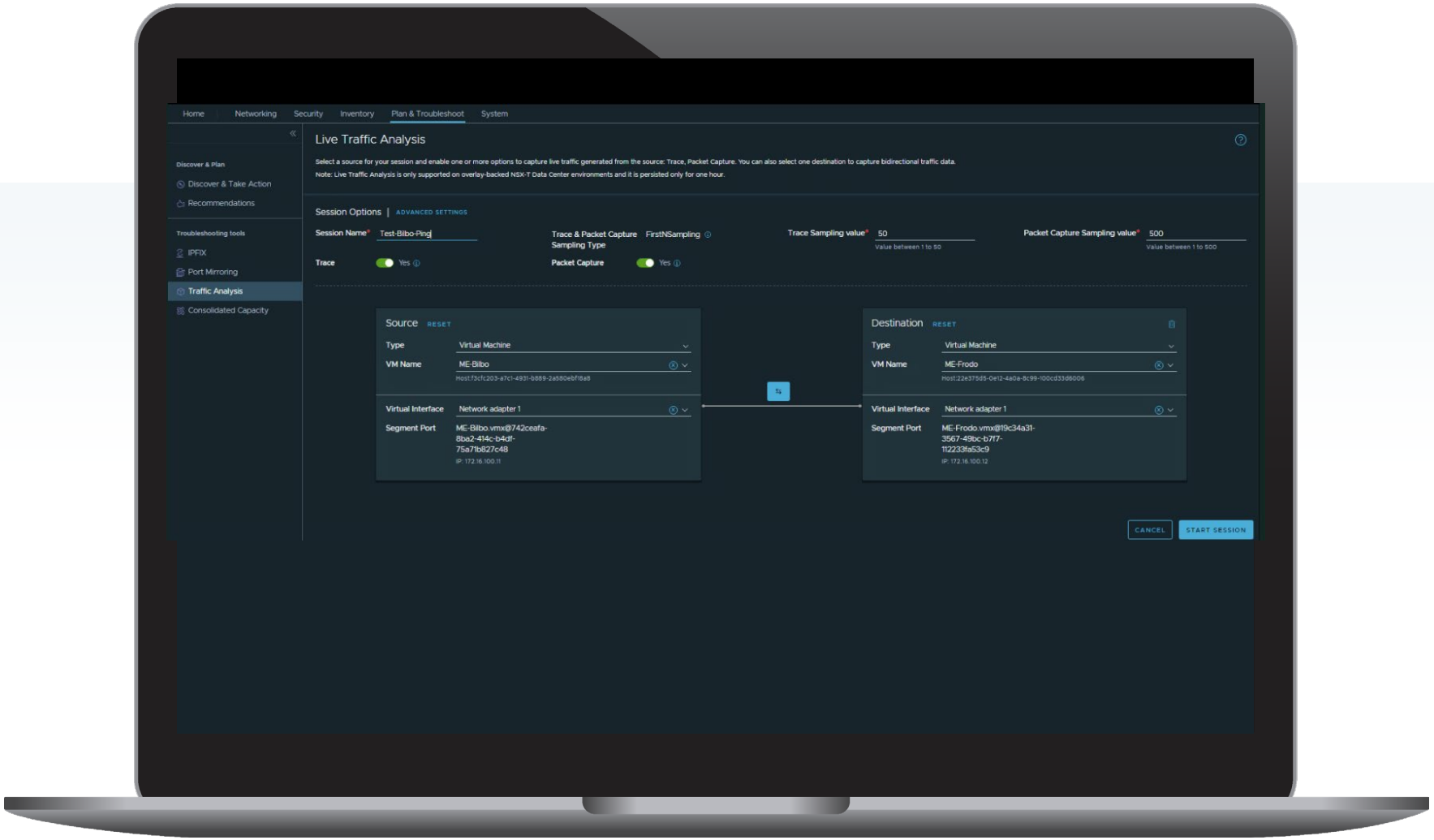
NSX Built in Tools

Traceflow



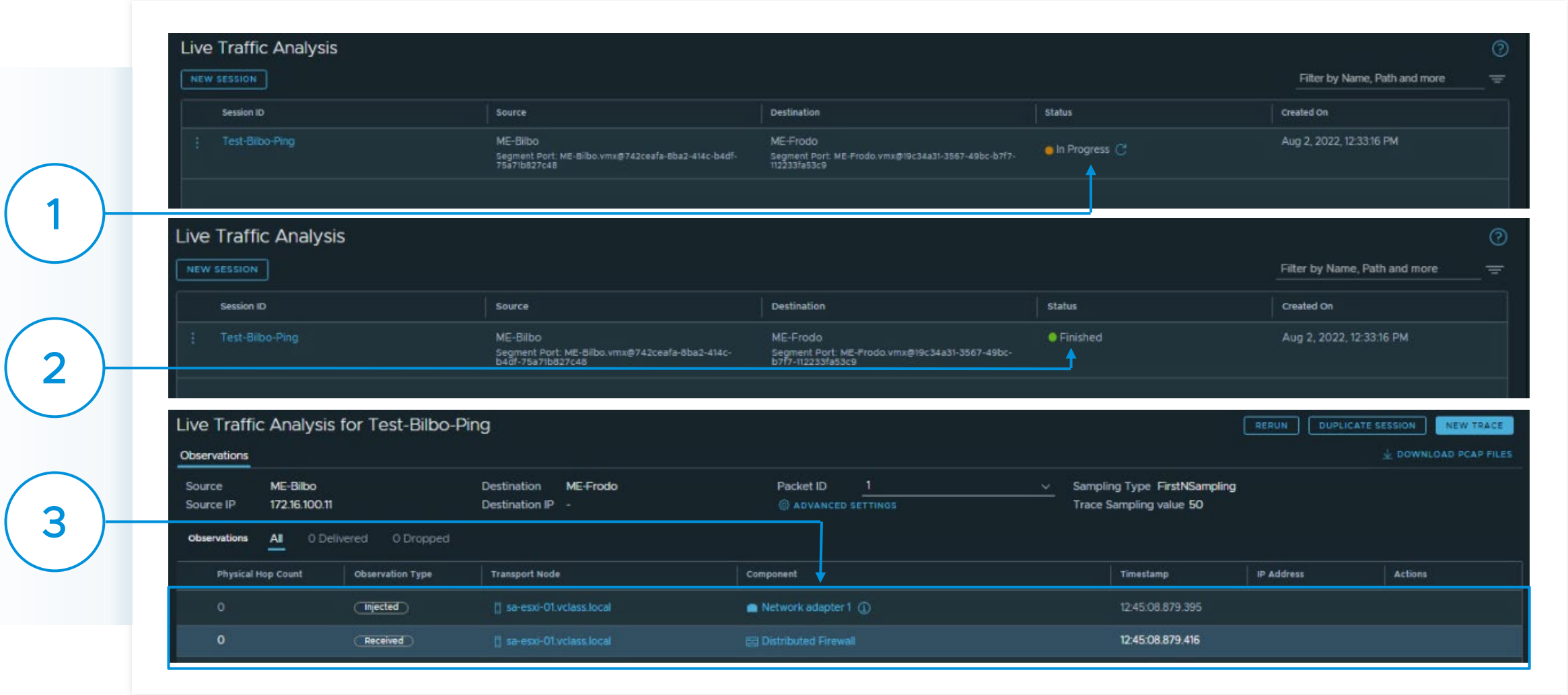
NSX Built in Tools

Live Traffic Analysis



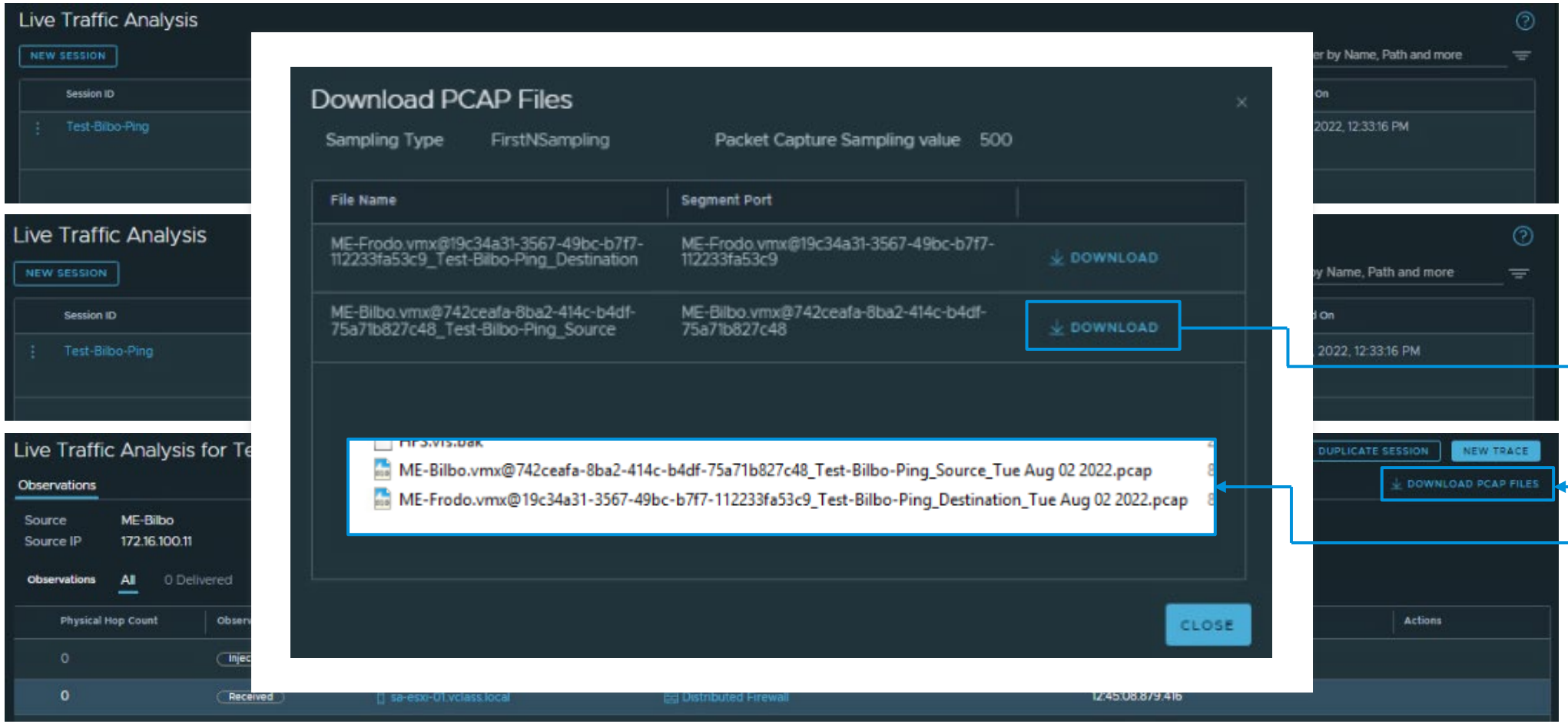
NSX Built in Tools

Live Traffic Analysis



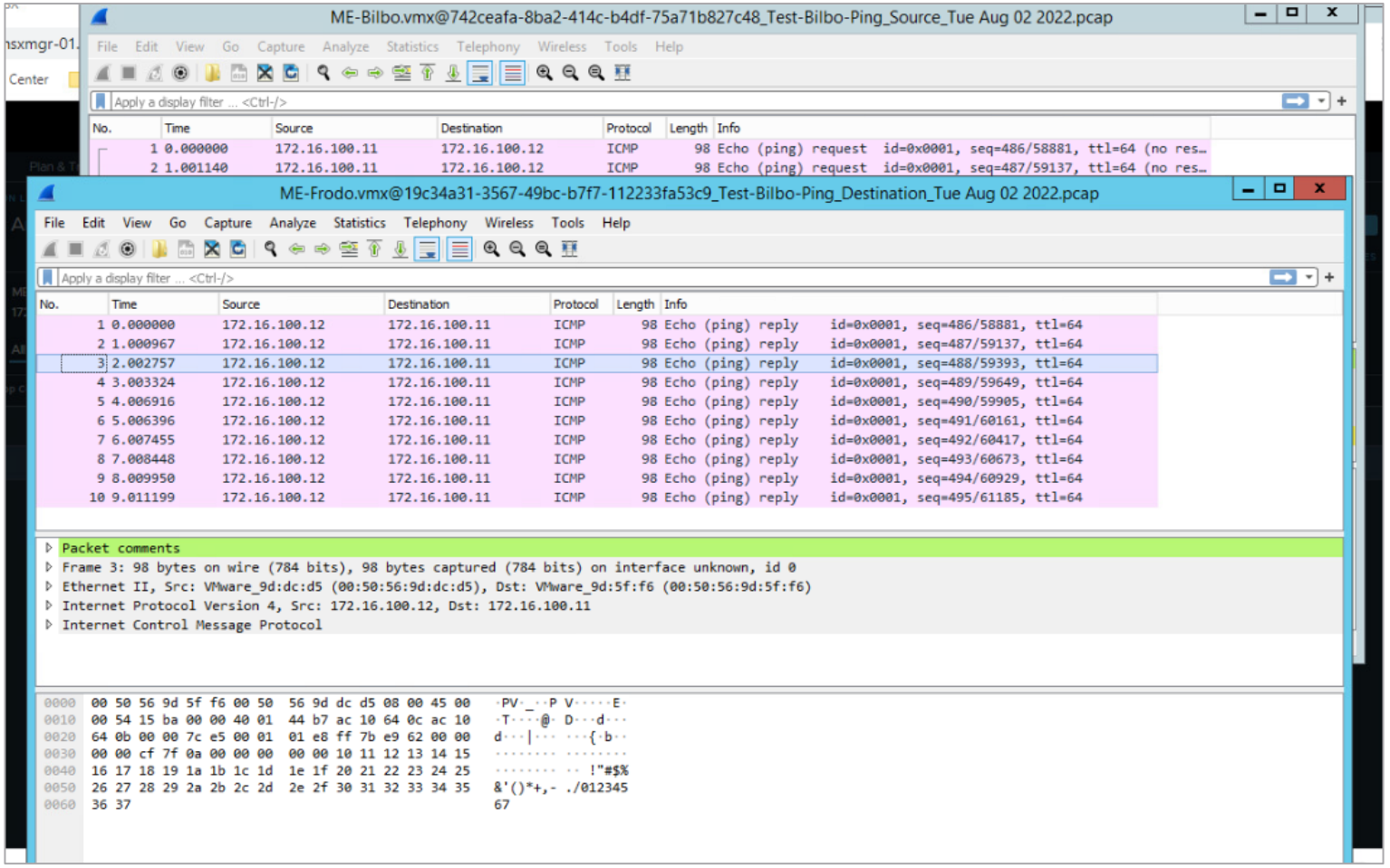
NSX Built in Tools

Live Traffic Analysis



NSX Built in Tools

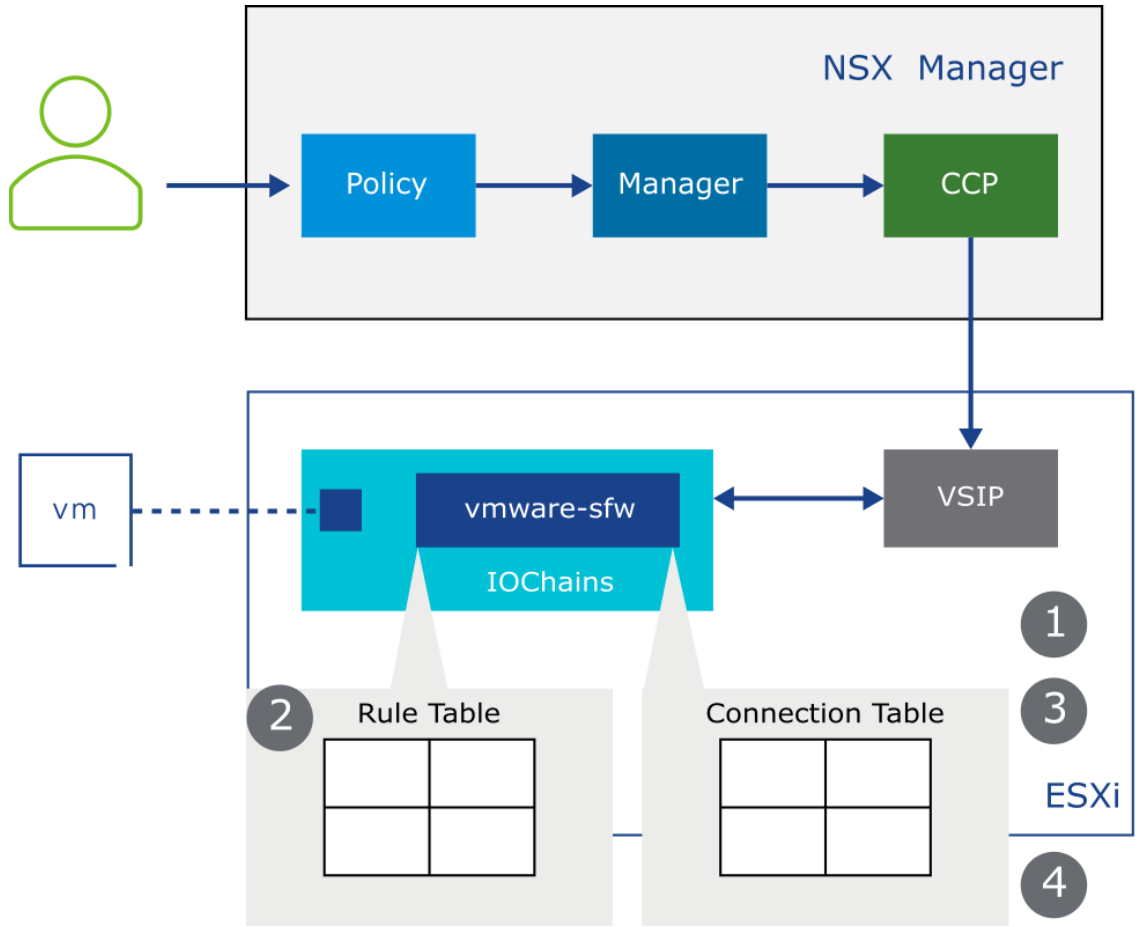
Live Traffic Analysis



Using the CLI to Validate Distributed Security Results

Using the CLI to Validate DFW Results

Is the DFW doing its job?



Using the CLI to Validate DFW Results

Common Commands to validate DFW on a vSphere transport node:

- **`summarize-dvfilter`** to find the filter name
- **`vsipioctl getrules –f <filter name>`**
- **`vsipioctl getaddrset –f <filter name>`**
- **`vsipioctl getflows –f <filter name>`**

Using the CLI to Validate DFW Results

```
[root@sa-esxi-01:~] summarize-dvfilter | grep -A 4 ME-Bil
world 808359 vmm0:ME-Bilbo vcUuid:'50 1d a4 8c cb f5 ce c7-b3 a6 85 25 20 ab ee d8'
 port 67108914 ME-Bilbo.eth0
  vNic slot 2
   name: nic-808359-eth0-vmware-sfw.2
   agentName: vmware-sfw
   state: IOChain Attached
[root@sa-esxi-01:~]
```

Using the CLI to Validate DFW Results

```
[root@sa-esxi-01:~] summarize-dvfilter | grep -A 4 ME-Bil
world 808359 vmm0:ME-Bilbo vcUuid:'50 1d a4 8c cb f5 ce c7-b3 a6 85 25 20 ab ee d8'
 port 67108914 ME-Bilbo.eth0
  vNic slot 2
   name: nic-808359-eth0-vmware-sfw.2
   agentName: vmware-sfw
   state: IOChain Attached
[root@sa-esxi-01:~]
```

```
[root@sa-esxi-01:~] vsipioctl getrules -f nic-808359-eth0-vmware-sfw.2
ruleset mainrs {
  # generation number: 0
  # realization time : 2022-08-02T18:56:55
  # PRE_FILTER rules
  rule 3050 at 1 inout protocol any from addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 to addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 reject;
  rule 3052 at 2 inout protocol tcp strict from not addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 to addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 port
22 with attribute profile 8caa3b4d-444a-4031-b057-4b3f51a05954 accept;
  rule 3053 at 3 inout protocol any from addrset 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 8081bb70-88e6-433c-8985-cfb05632f126 accept;
  rule 3055 at 4 inout protocol any from addrset 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 5b71c129-072a-4856-b34f-db649c6d4195 accept;
  rule 3056 at 5 inout protocol any from any to any reject;
  # FILTER (APP Category) rules
  rule 3 at 1 inout inet6 protocol ipv6-icmp icmptype 135 from any to any accept;
  rule 3 at 2 inout inet6 protocol ipv6-icmp icmptype 136 from any to any accept;
  rule 4 at 3 inout protocol udp from any to any port {67, 68} accept;
  rule 2 at 4 inout protocol any from any to any accept;
  # IDP rules
  rule 3061 at 1 inout protocol any from any to any with ids profile 8a7465b3-363c-46ad-8117-7e702fce4d62 idp_protect;
```

Using the CLI to Validate DFW Results

```
[root@sa-esxi-01:~] summarize-dvfilter | grep -A 4 ME-Bil
world 808359 vmm0:ME-Bilbo vcUuid:'50 1d a4 8c cb f5 ce c7-b3 a6 85 25 20 ab ee d8'
 port 67108914 ME-Bilbo.eth0
  vNic slot 2
   name: nic-808359-eth0-vmware-sfw.2
   agentName: vmware-sfw
   state: IOChain Attached
[root@sa-esxi-01:~]
```

```
[root@sa-esxi-01:~] vsipioctl getaddrsets -f nic-808359-eth0-vmware-sfw.2
addrset is shared for this filter
global addrset
addrset 0236f0d8-1735-4850-a3a0-ed1273dcdcc2 {
ip 172.16.200.11,
ip 172.16.200.13,
mac 00:50:56:9d:03:97,
mac 00:50:56:9d:0d:4e,
}
addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 {
ip 172.16.100.11,
ip 172.16.100.13,
mac 00:50:56:9d:5f:f6,
mac 00:50:56:9d:8c:2d,
}
addrset 5b71c129-072a-4856-b34f-db649c6d4195 {
ip 172.16.100.11,
ip 172.16.100.12,
ip 172.16.100.13,
mac 00:50:56:9d:5f:f6,
mac 00:50:56:9d:8c:2d,
mac 00:50:56:9d:dc:d5,
```

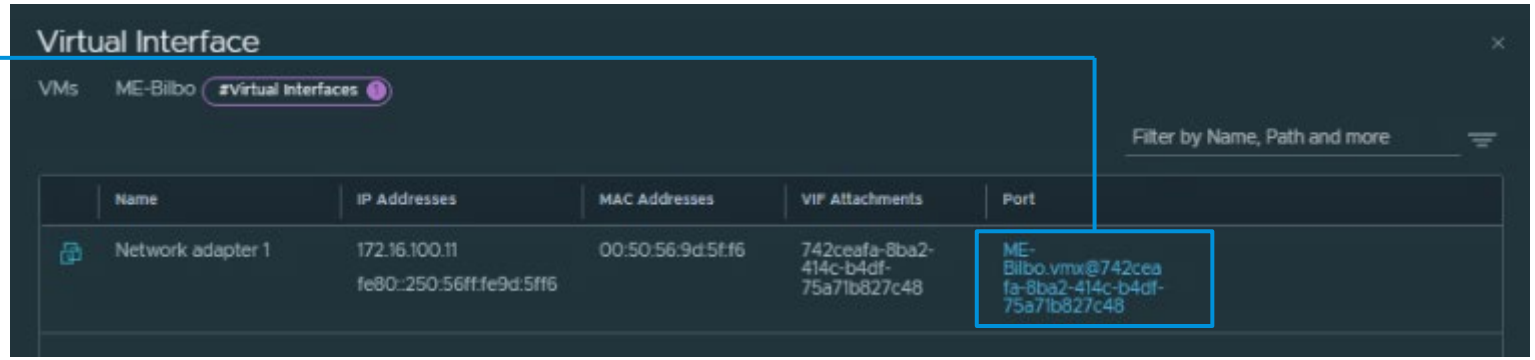
Using the CLI to Validate DFW Results

Find information if the Host Credentials are not available – NSX Manager

```
sa-nsxmgr-01> get nodes
Tue Aug 02 2022 UTC 20:53:57.870
UUID                                   Type  Display Name
ece51cee-4ac9-48c1-9735-ff065512440c   edg   sa-nsxedge-01
f3cfc203-a7c1-4931-b889-2a580ebf18a8   esx   sa-esxi-01.vclass.local
22e375d5-0e12-4a0a-8c99-100cd33d6006   esx   sa-esxi-02.vclass.local
8cfe9d5e-29db-4008-8021-9833871fa8a0   kvm   sa-kvm-01
bdb81d42-7341-5abc-c3fc-4fa583fedea8   mgr   sa-nsxmgr-01

sa-nsxmgr-01> on f3cfc203-a7c1-4931-b889-2a580ebf18a8 exec get firewall vifs
------------------------------------------------------------------------------
f3cfc203-a7c1-4931-b889-2a580ebf18a8  esx  sa-esxi-01.vclass.local
------------------------------------------------------------------------------
Tue Aug 02 2022 UTC 20:54:21.235
                          Firewall VIFs
------------------------------------------------------------------------

VIF count: 7
 1   0c064897-ae2d-4271-8189-0b97b4c641ca
 2   742ceafa-8ba2-414c-b4df-75a71b827c48
 3   82269fe3-544a-4fb6-9bba-3ad545f462d6
 4   a1e34624-ece2-4571-afca-ec18249e1fbb
 5   a29ea912-1175-46c3-8fcc-457de623c342
 6   e23e818b-df86-4c7e-b734-808cb807c5ef
 7   e5b2c494-7efe-4ed3-9e98-a15dcb72e0a2
```



Using the CLI to Validate DFW Results

Find information if the Host Credentials are not available – NSX Manager

```
sa-nsxmgr-01> on f3cfc203-a7c1-4931-b889-2a580ebf18a8 exec get firewall 742ceafa-8ba2-414c-b4df-75a71b827c48 ruleset rules
------------------------------------------------------------------------------------------------------------------------------------------------------------
f3cfc203-a7c1-4931-b889-2a580ebf18a8  esx  sa-esxi-01.vclass.local
------------------------------------------------------------------------------------------------------------------------------------------------------------
Tue Aug 02 2022 UTC 20:53:17.162
                            Firewall Rules
-----------------------------------------------------------------

VIF UUID : 742ceafa-8ba2-414c-b4df-75a71b827c48
  Ruleset UUID : de6f9262-f6ca-4518-804a-5d25b2c639ca
  Rule count : 1
    rule 3061 inout protocol any from any to any with ids profile 8a7465b3-363c-46ad-8117-7e702fce4d62 idp_protect;

  Ruleset UUID : 02ed5703-a0e9-4d29-b152-3dd07d66c3ec
  Rule count : 5
    rule 3050 inout protocol any from addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 to addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 in pre_filter reject;
    rule 3052 inout protocol tcp strict from not addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 to addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 port 22 with attribute
 profile 8caa3b4d-444a-4031-b057-4b3f51a05954 in pre_filter accept;
    rule 3053 inout protocol any from addrset 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 8081bb70-88e6-433c-8985-cfb05632f126 in pre_filter accept;
    rule 3055 inout protocol any from addrset 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 5b71c129-072a-4856-b34f-db649c6d4195 in pre_filter accept;
    rule 3056 inout protocol any from any to any in pre_filter reject;

  Ruleset UUID : ffffffff-8a04-4924-a5b4-54d30e81befe
  Rule count : 4
    rule 3 inout inet6 protocol ipv6-icmp icmptype 135 from any to any accept;
    rule 3 inout inet6 protocol ipv6-icmp icmptype 136 from any to any accept;
    rule 4 inout protocol udp from any to any port {67, 68} accept;
    rule 2 inout protocol any from any to any accept;

  Ruleset UUID : ffffffff-35f8-4611-a40f-545432e3119a
  Rule count : 1
    rule 1 inout ethertype any stateless from any to any accept;
```

vmware EXPLORE

Thank You