AWS Immersion Day
LAB 5

SECURITY: DISTRIBUTED FIREWALL

Brad Hedlund

Principal Solutions Architect, Aviatrix Systems

Lab 4 Recap

Segmentation

PRODUCTION
SHARED
DEV
PCI
10.51.0.0/16
Spoke 1
Jump Instance
10.51.0.10
SAP1
10.52.0.0/16
Spoke 2
10.52.0.10
SAP2
10.52.0.0/16
Spoke 3
10.53.0.10
SAP3
10.0.0.0/16
VPC A
EC2-A
10.1.0.0/16
VPC B
EC2-B
Controller VPC
Aviatrix CoPilot
Aviatrix Controller
Transit
10.50.0.0/16
10.2.0.0/16
VPC C (Transit)
EC2-C
AWS us-west-2
AWS us-east-1

Segmentation either ALLOWS or PREVENTS all traffic between domains.

Did you know every Aviatrix Spoke Gateway is a stateful L4 Firewall? Let's use that to get firewalls everywhere and apply granular security controls… (next)

Lab 5 Intro

Distributed Firewall

PRODUCTION
SHARED
DEV
PCI
10.51.0.0/16
Spoke 1
Jump Instance
10.51.0.10
SAP1
10.52.0.0/16
Spoke 2
10.52.0.10
SAP2
10.52.0.0/16
Spoke 3
10.53.0.10
SAP3
10.0.0.0/16
VPC A
EC2-A
10.1.0.0/16
VPC B
EC2-B
Controller VPC
Aviatrix CoPilot
Aviatrix Controller
TCP 8000 ONLY
Transit
10.50.0.0/16
10.2.0.0/16
VPC C (Transit)
EC2-C
AWS us-west-2
AWS us-east-1

Our segmentation allows all communication between PROD and SHARED

In this Lab we will allow our SAP instances in PROD to talk to SAP3 in SHARED **only on TCP port 8000** – without using expensive L7 firewalls. Let's configure the Aviatrix Spoke Gateways as one big **Distributed Firewall** !

Lab 5: Distributed Firewall: Step 5.0

Create SmartGroups

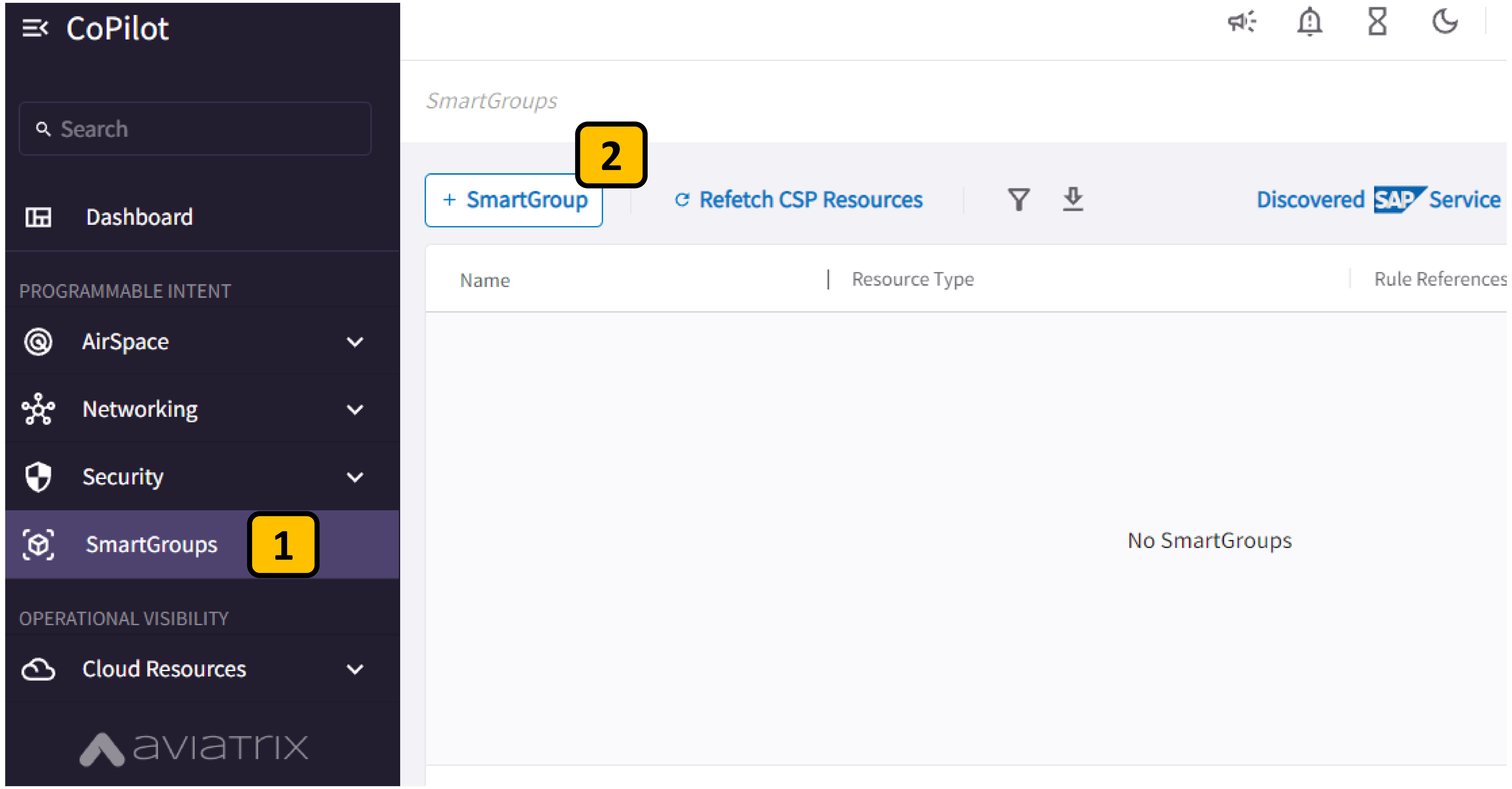
SmartGroups are way to logically group resources in your cloud network. We can use these SmartGroups to define firewall policies.

Let's create a SmartGroups and call them **SAP-App1 and SAP-App2**

We'll put instances SAP1 and SAP2 in the group using a EC2 instance tags
Application = SAP-App1 (SAP1)
Application = SAP-App2 (SAP2)

Click on **SmartGroups** 1

Click **+ SmartGroup** 2



Lab 5: Distributed Firewall: Step 5.1

Create SmartGroups

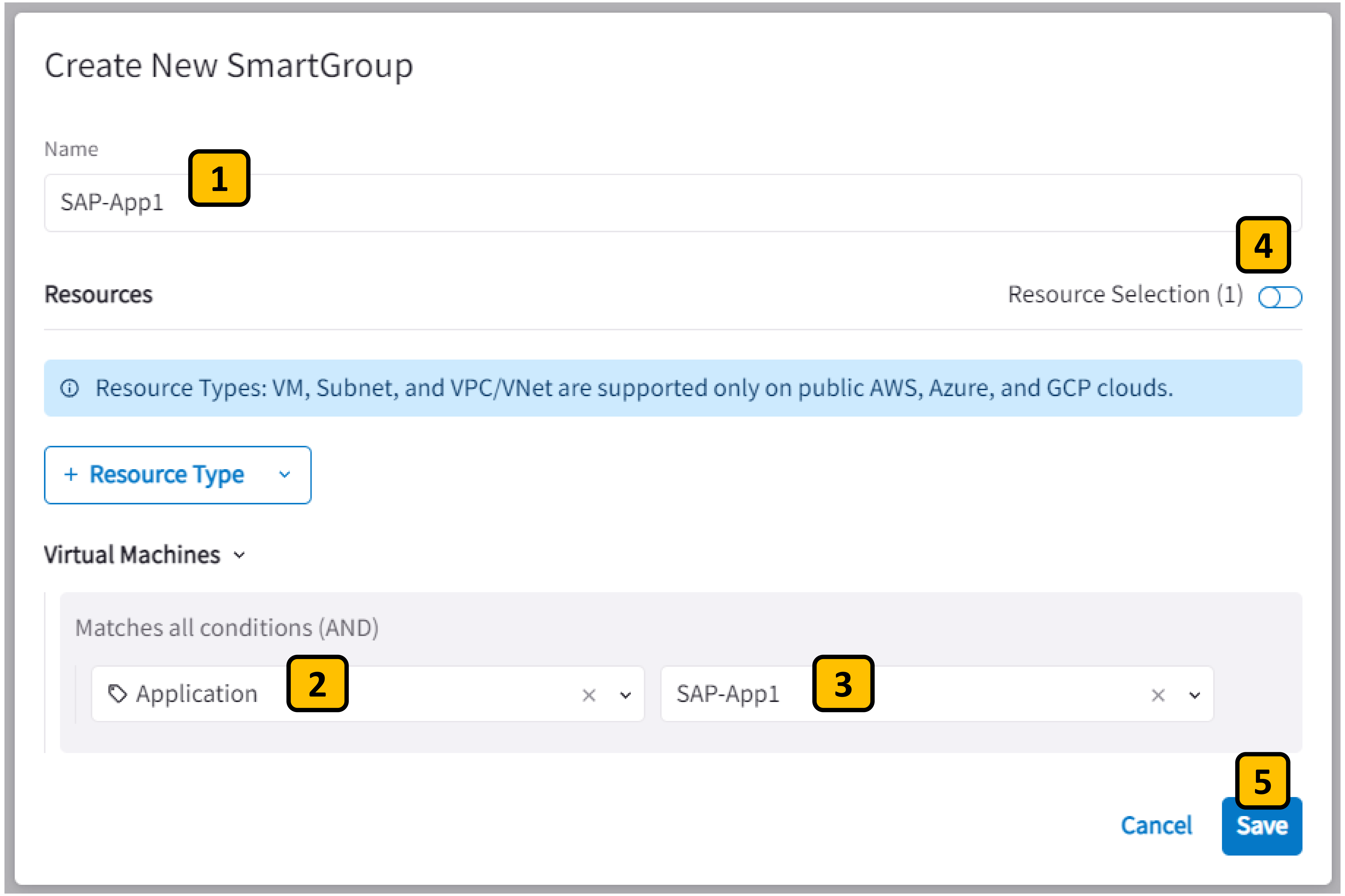
Name the SmartGroup:
SAP-App1 1

Under Virtual Machines, select the CSP Tag **Application** 2

Match on the tag value **SAP-App1** 3

If you're curious, click **Resource Selection** to make sure the instance SAP1 matches your criteria. 4

Click **Save** 5



Create New SmartGroup

Name: SAP-App1 1

Resources

Resource Selection (1) 4

ⓘ Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.

Matches all conditions (AND)

Application 2 — SAP-App1 3

Lab 5: Distributed Firewall: Step 5.2

Create SmartGroups

Create another SmartGroup

Name the SmartGroup:
SAP-App2 1

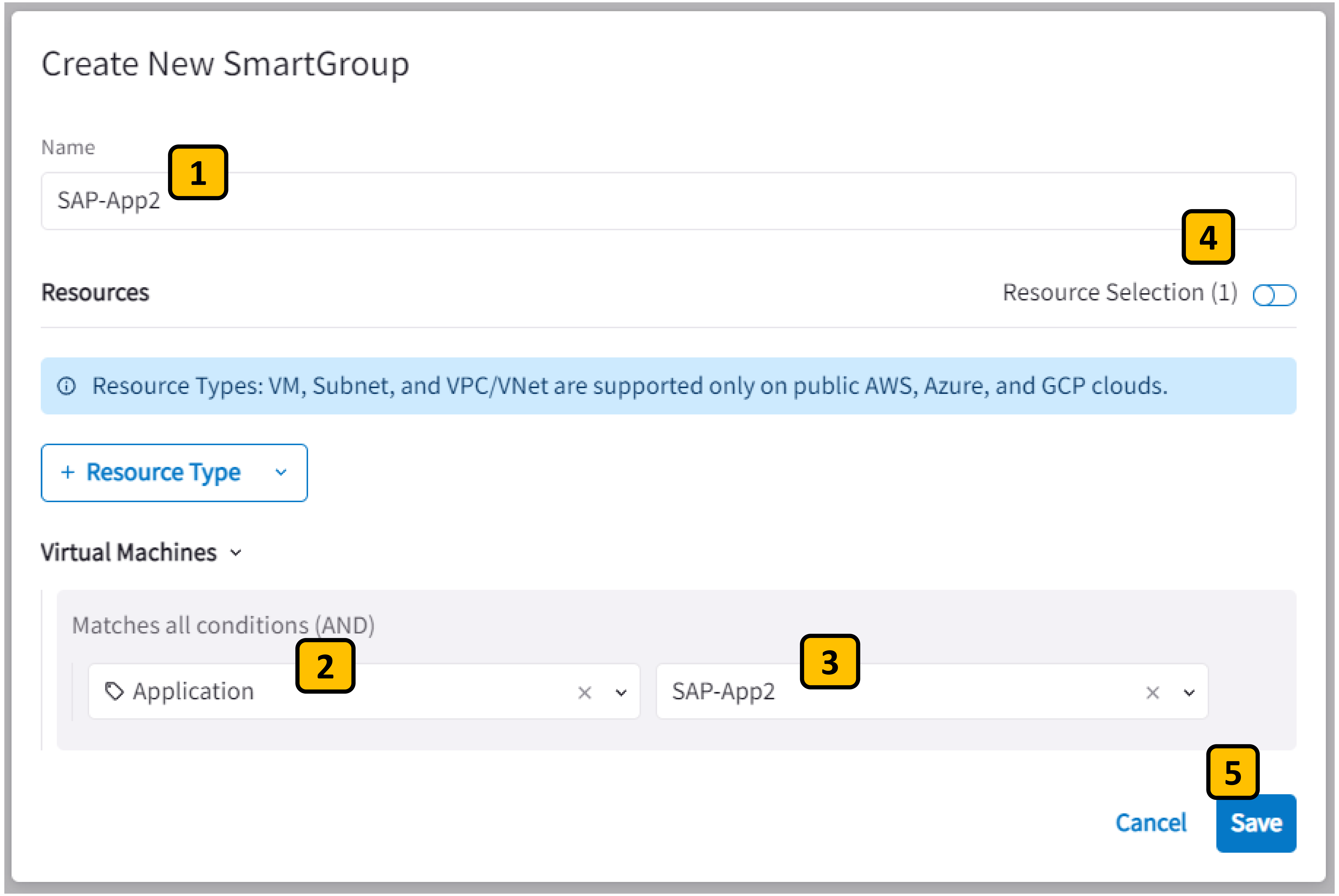
Under Virtual Machines, select the CSP Tag **Application** 2

3

Match on the tag value **SAP-App2**

If you're curious, click **Resource Selection** to make sure the instance SAP2 matches your criteria. 4

Click **Save** 5



Create New SmartGroup

Name: SAP-App2

Resources

Resource Selection (1)

ⓘ Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.

Virtual Machines

Matches all conditions (AND)

Application: SAP-App2

Lab 5: Distributed Firewall: Step 5.3

Create SmartGroups

Create another SmartGroup

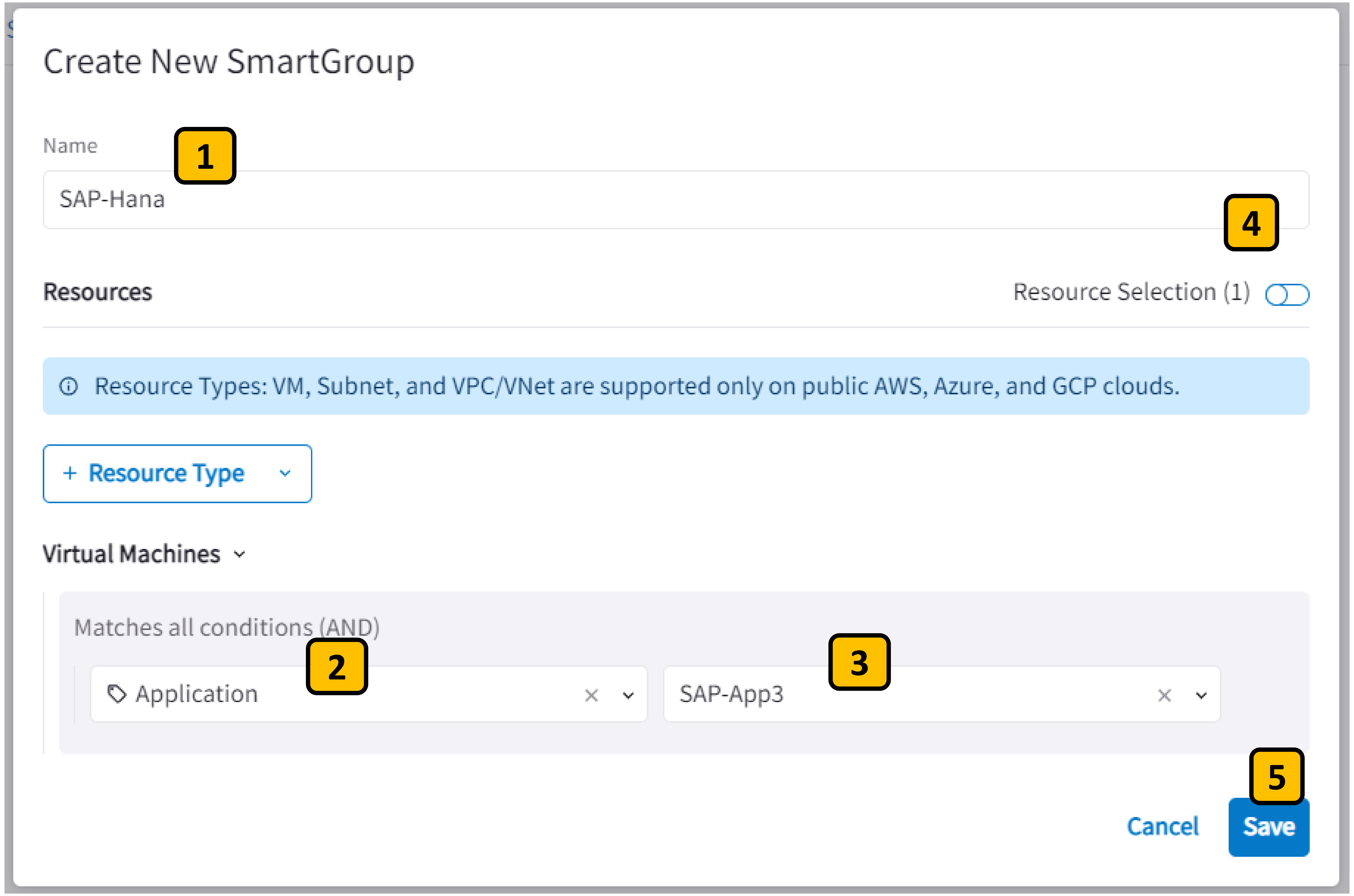
Name the SmartGroup:
SAP-Hana 1

Under Virtual Machines, select the CSP Tag **Application** 2

3
Match on the tag value **SAP-App3**

If you're curious, click **Resource Selection** to make sure the instance SAP3 matches your criteria. 4

Click **Save** 5



Create New SmartGroup

Name: SAP-Hana

Resources

Resource Selection (1)

ⓘ Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.

Virtual Machines

Matches all conditions (AND)

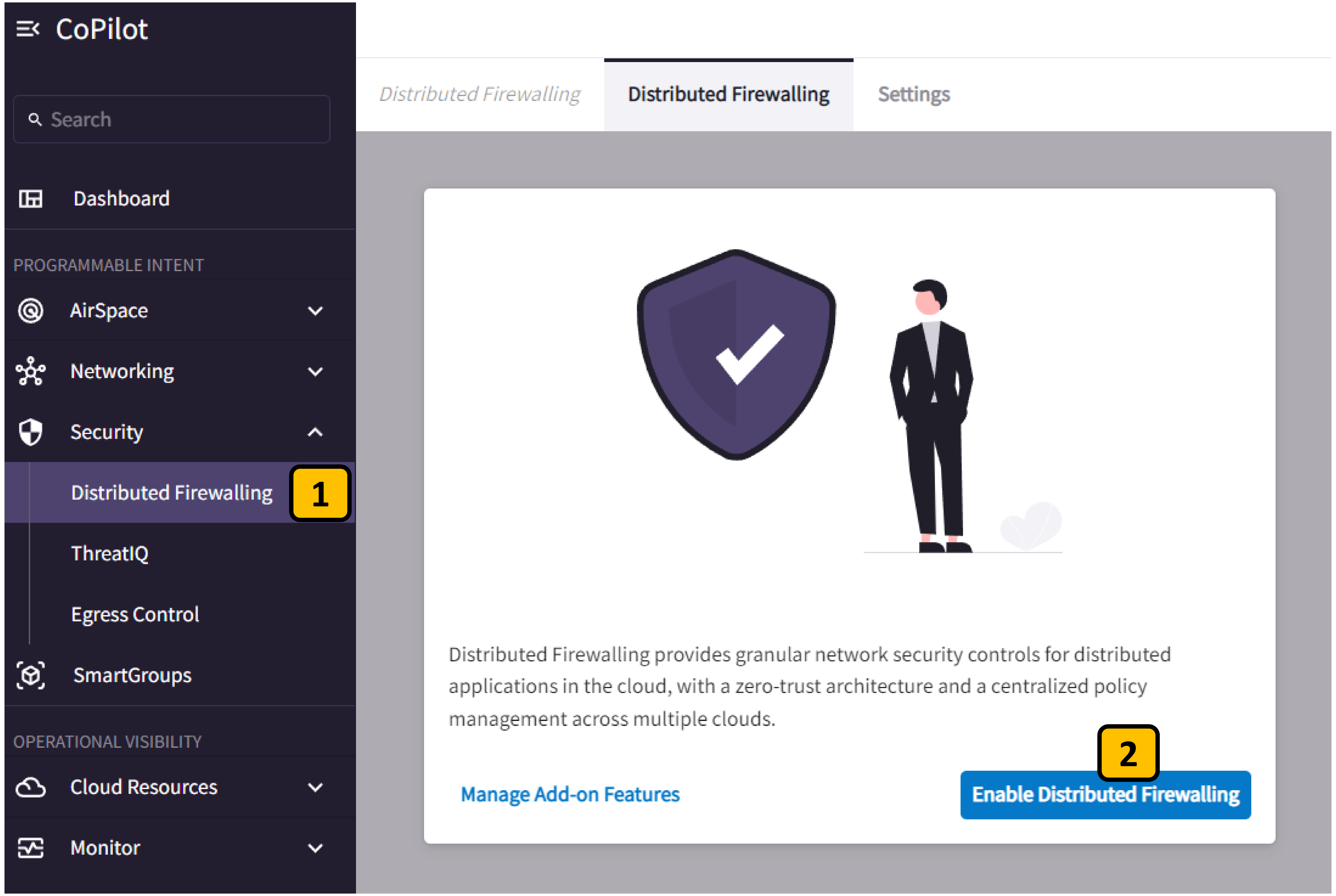
Application × SAP-App3 ×

Lab 5: Distributed Firewall: Step 5.4

Enable Distributed Firewall

Go to Security > **Distributed Firewalling** 1

Enable the Distributed Firewalling Add-on feature. 2



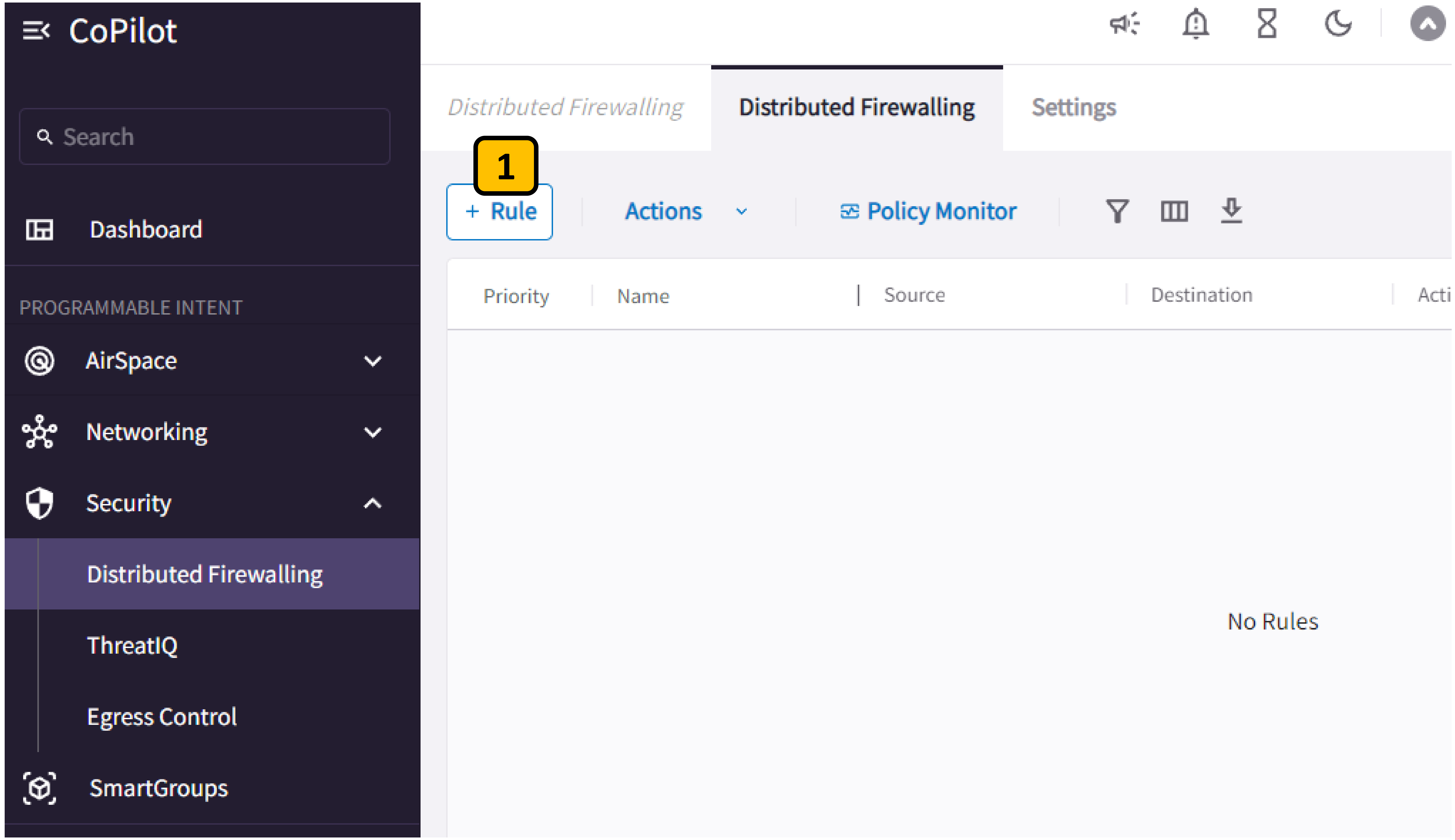
Distributed Firewalling provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

Lab 5: Distributed Firewall: Step 5.5

Create Distributed Firewalling Rules

Now let’s first create a rule that says our SAP SmartGroups can access the internet.

Click **+ Rule** 1



Lab 5: Distributed Firewall: Step 5.6

Create Distributed Firewalling Rules

Give the rule the name **Allow-internet** 1

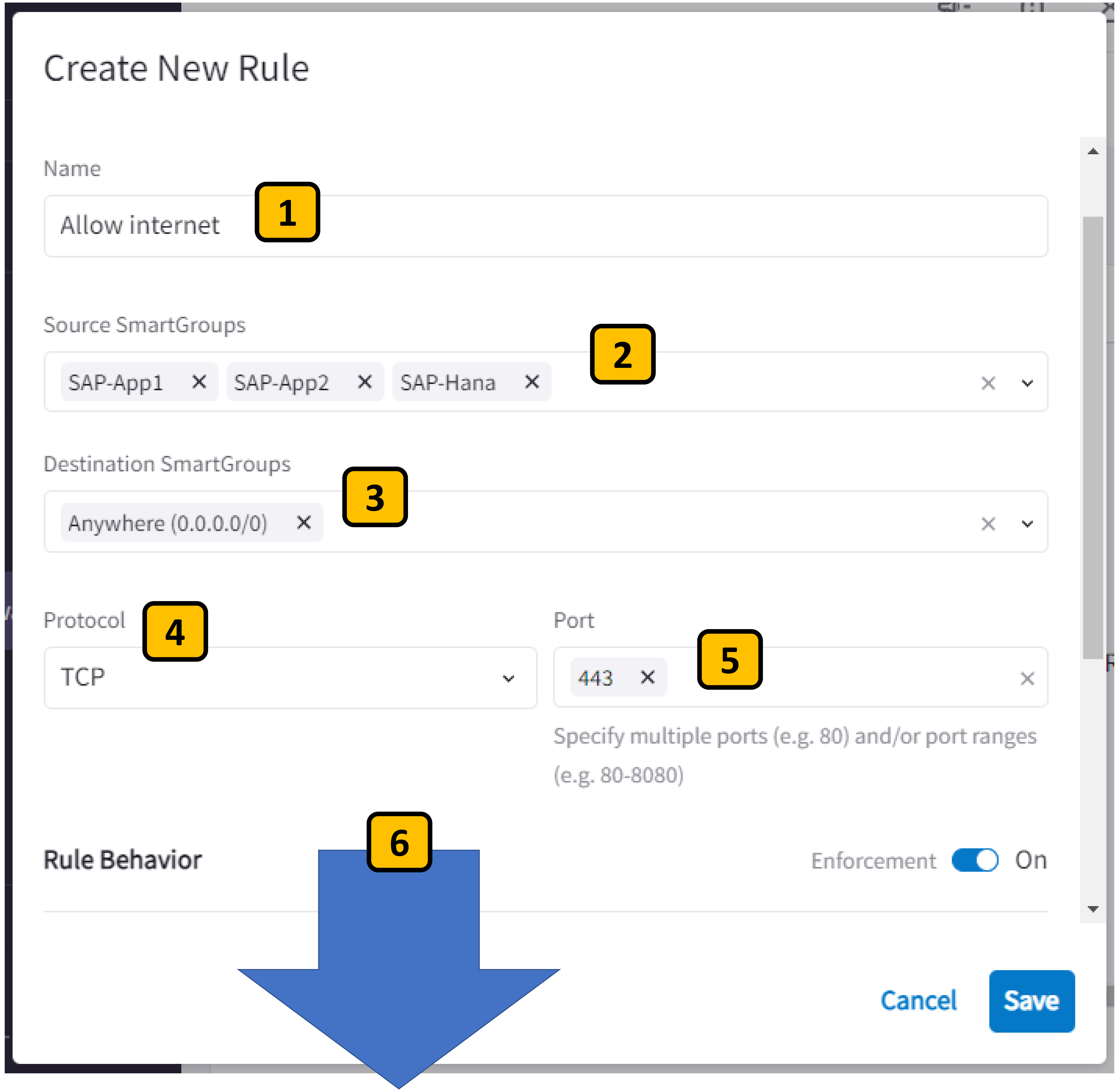
For Source SmartGroups select our three groups, SAP-App1, SAP-App2, and SAP-Hana 2

For Destination SmartGroups select **Anywhere (0.0.0.0/0)** 3

Select Protocol **TCP** 4

Type in Port **443** 5

Scroll down 6



Create New Rule

Name: Allow internet 1

Source SmartGroups: SAP-App1 ✕ SAP-App2 ✕ SAP-Hana ✕ 2

Destination SmartGroups: Anywhere (0.0.0.0/0) ✕ 3

Protocol: TCP 4

Port: 443 ✕ 5

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior 6

Enforcement: On

Lab 5: Distributed Firewall: Step 5.7

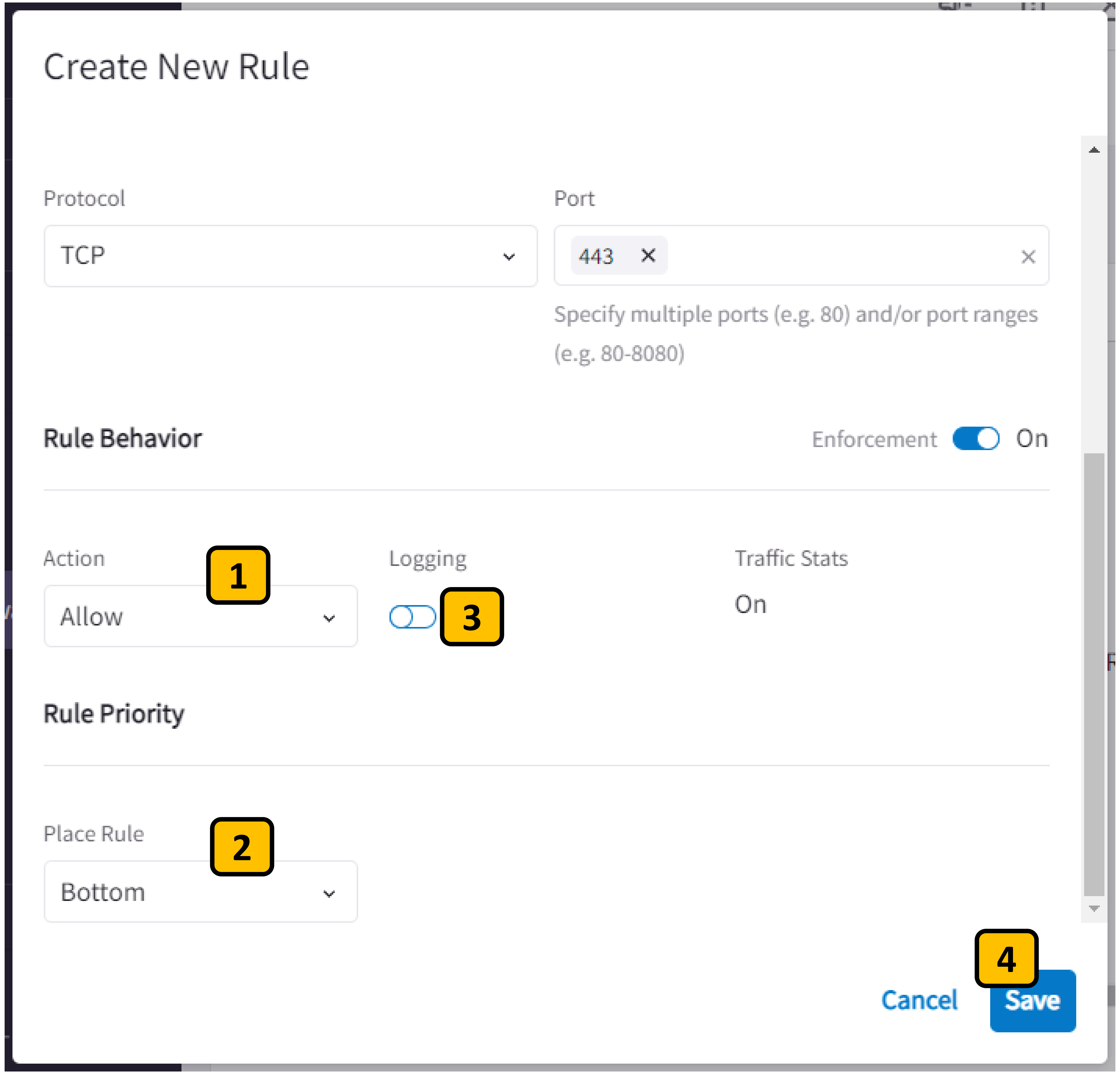
Create Distributed Firewalling Rules

Make sure Action is set to **Allow** 1

Set **Bottom** for Place Rule 2

Make sure Logging is set to **ON** 3

Click **Save** 4



Create New Rule

Protocol: TCP

Port: 443

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement On

Action: Allow

Logging

Traffic Stats: On

Rule Priority

Place Rule: Bottom

Lab 5: Distributed Firewall: Step 5.8

Create Distributed Firewalling Rules

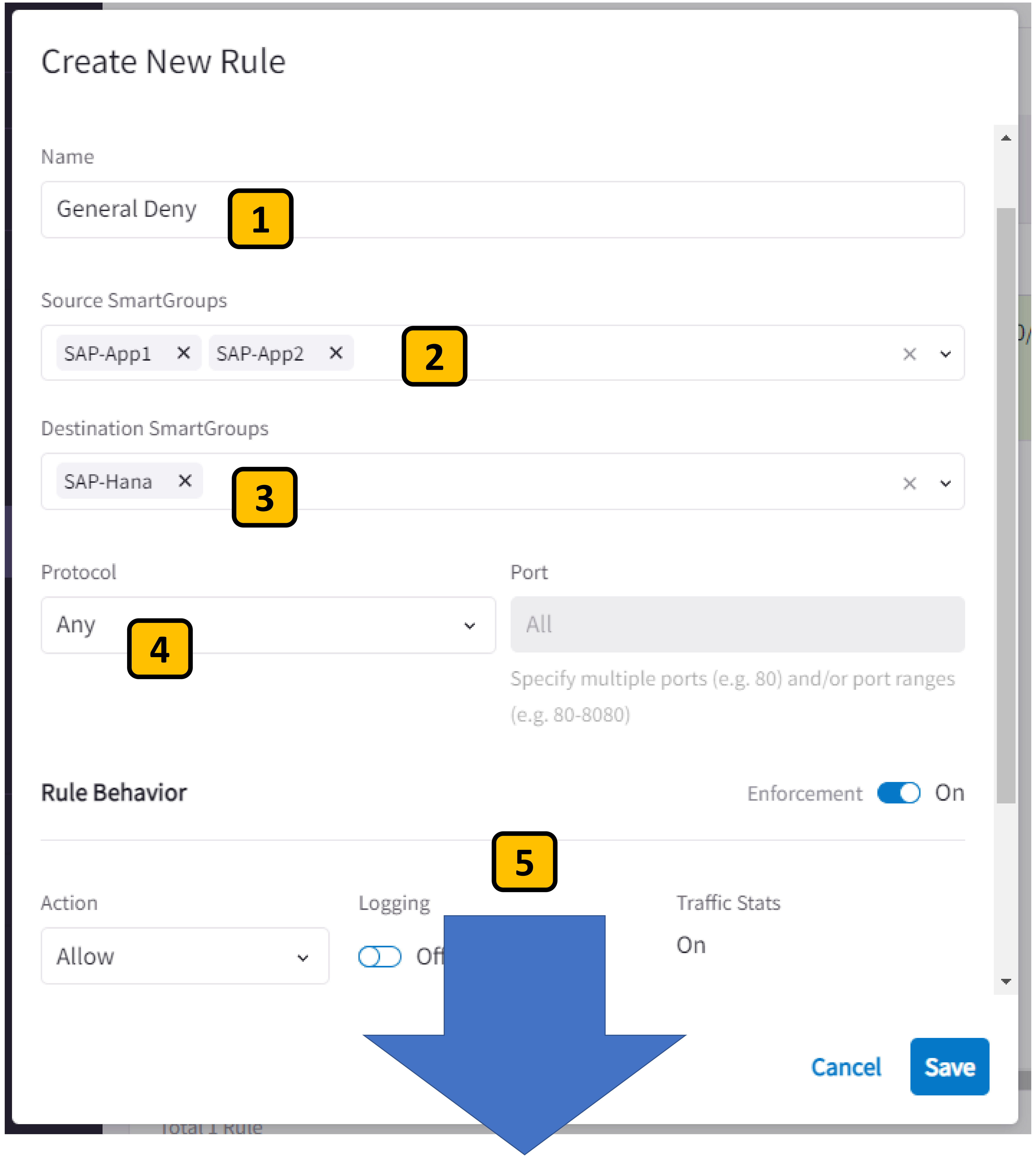
Create another rule called **General-Deny** 1

For Source SmartGroups select **SAP-App1** and **SAP-App2** 2

For Destination SmartGroups select **SAP-Hana** 3

Protocol **Any** 4

Scroll down 5



Create New Rule

Name: General Deny 1

Source SmartGroups: SAP-App1 ✕ SAP-App2 ✕ 2

Destination SmartGroups: SAP-Hana ✕ 3

Protocol: Any 4

Port: All

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement: On

5

Action: Allow

Logging: Off

Traffic Stats: On

Lab 5: Distributed Firewall: Step 5.9

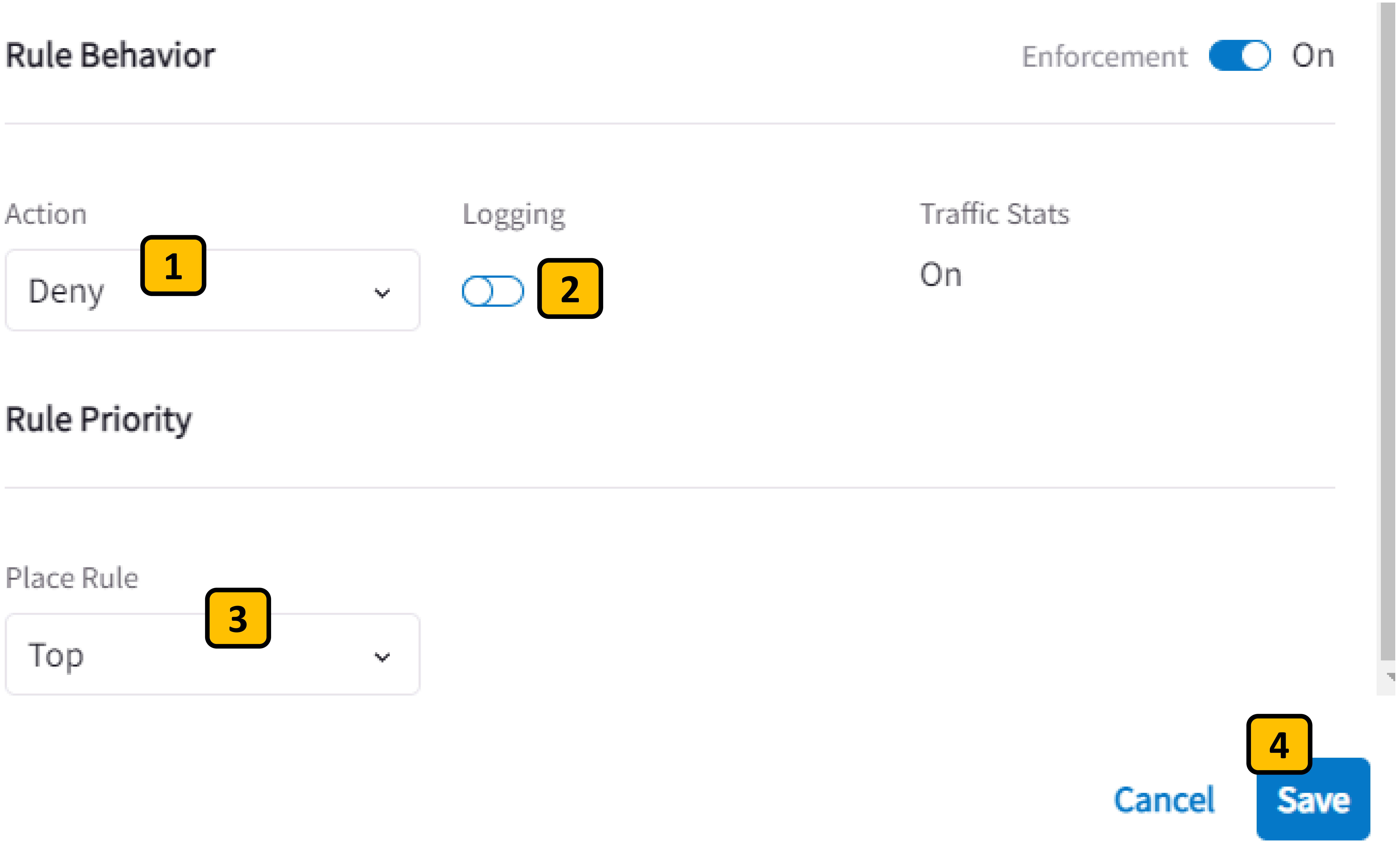
Create Distributed Firewalling Rules

Make sure Action is set to **Deny** 1

Make sure Logging is set to **ON** 2

Set **Top** for Place Rule 3

Click **Save** 4



Rule Behavior

Enforcement: On

Action: Deny 1

Logging 2

Traffic Stats: On

Rule Priority

Place Rule: Top 3

Lab 5: Distributed Firewall: Step 5.10

Create Distributed Firewalling Rules

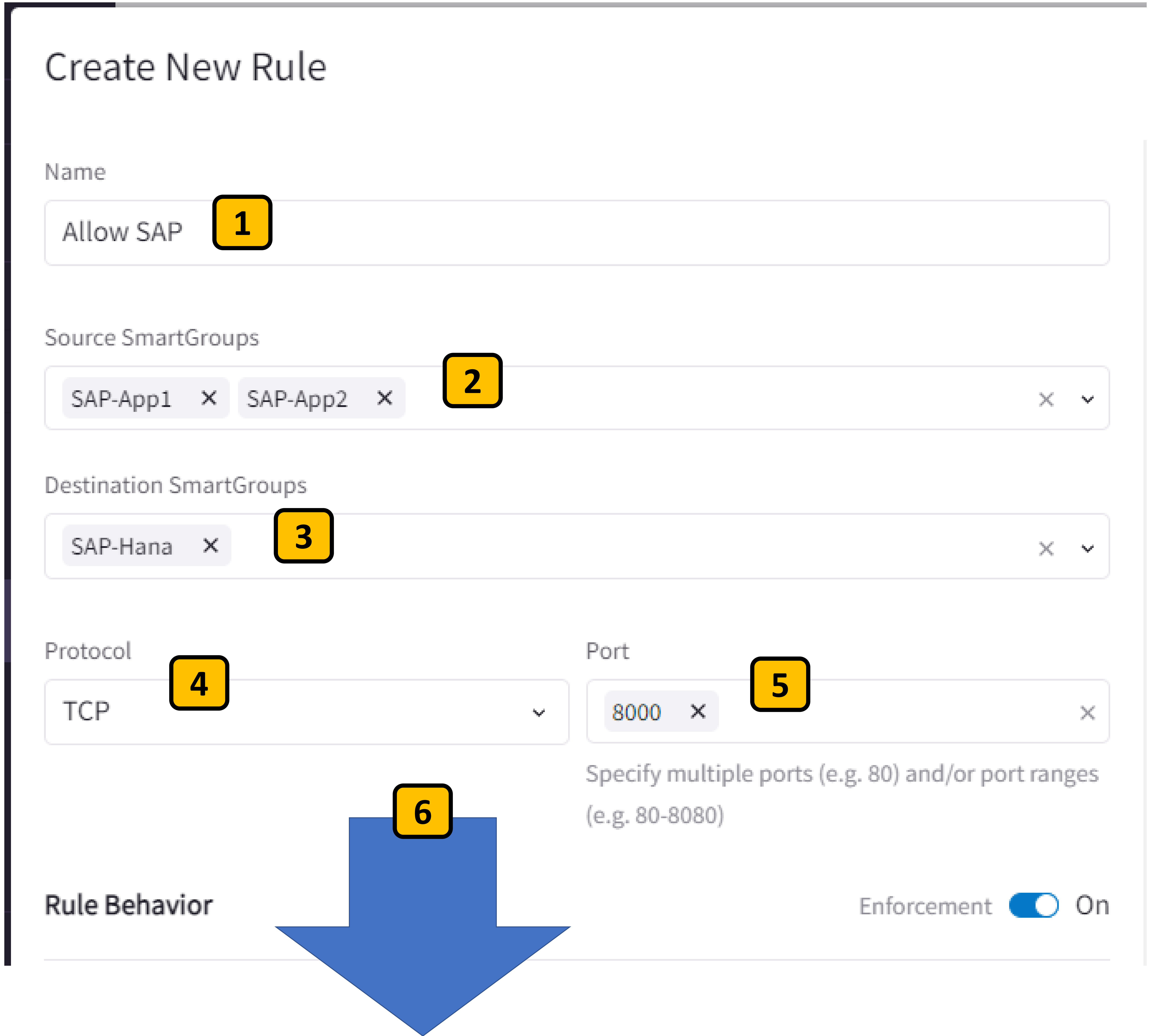
Create another rule called **Allow-SAP** 1

For Source SmartGroups select **SAP-App1** and **SAP-App2** 2

For Destination SmartGroups select **SAP-Hana** 3

Protocol **TCP** 4
Port **8000** 5

Scroll down 6



Create New Rule

Name: Allow SAP 1

Source SmartGroups: SAP-App1 ✕ SAP-App2 ✕ 2

Destination SmartGroups: SAP-Hana ✕ 3

Protocol: TCP 4

Port: 8000 ✕ 5

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

6

Rule Behavior

Enforcement On

Lab 5: Distributed Firewall: Step 5.11

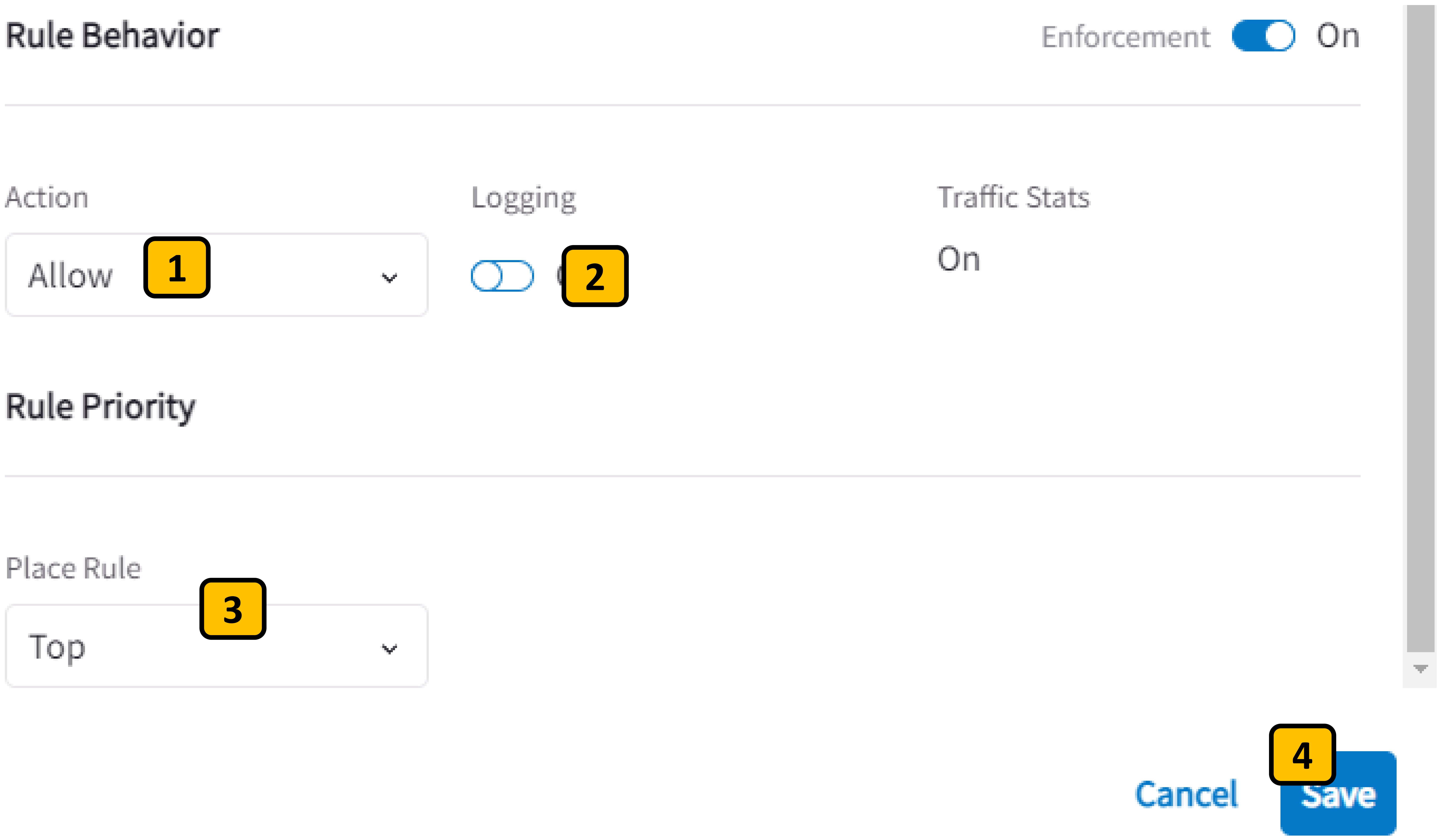
Create Distributed Firewalling Rules

Make sure Action is set to **Allow** 1

Make sure Logging is set to **ON** 2

Set **Top** for Place Rule 3

Click **Save** 4



Rule Behavior

Enforcement On

Action: Allow

Logging:

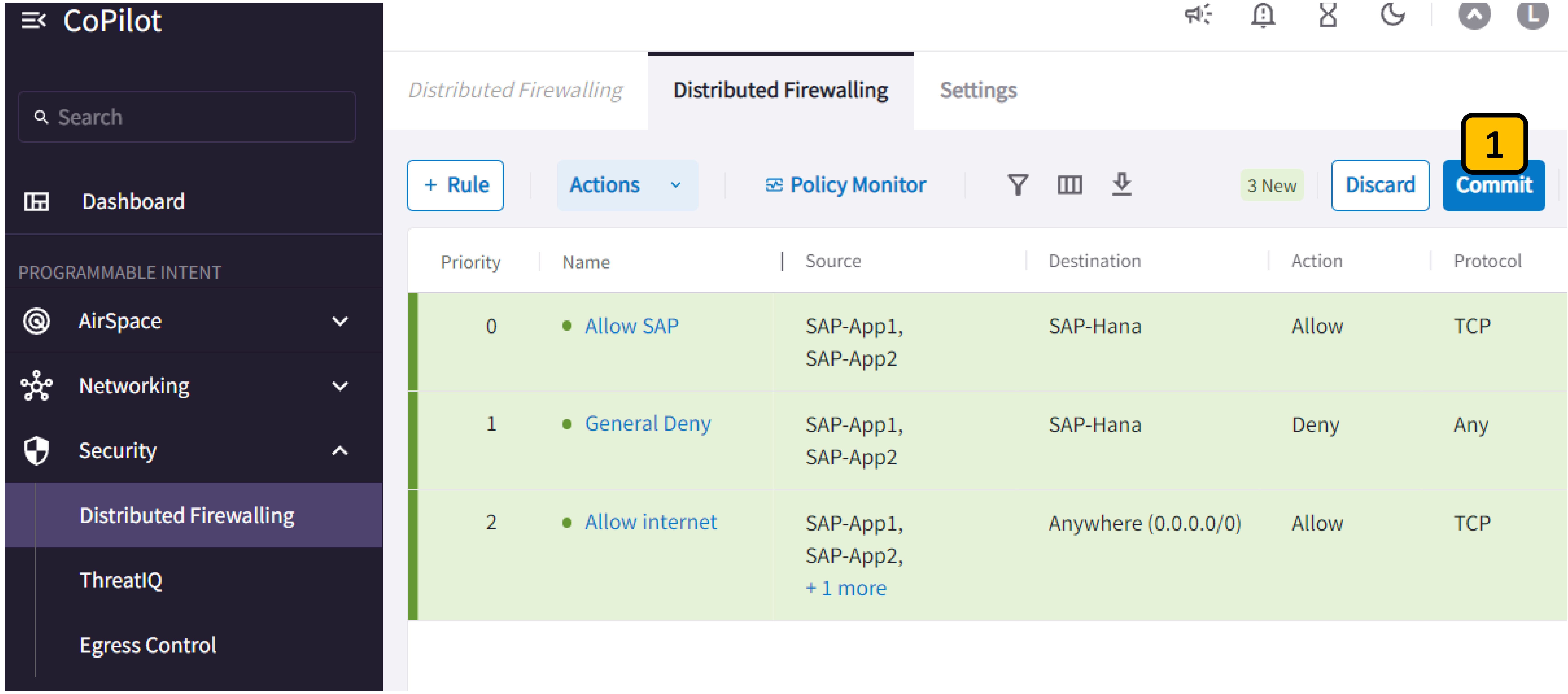
Traffic Stats: On

Rule Priority

Place Rule: Top

Lab 5: Distributed Firewall: Step 5.5

Create Distributed Firewalling Rules



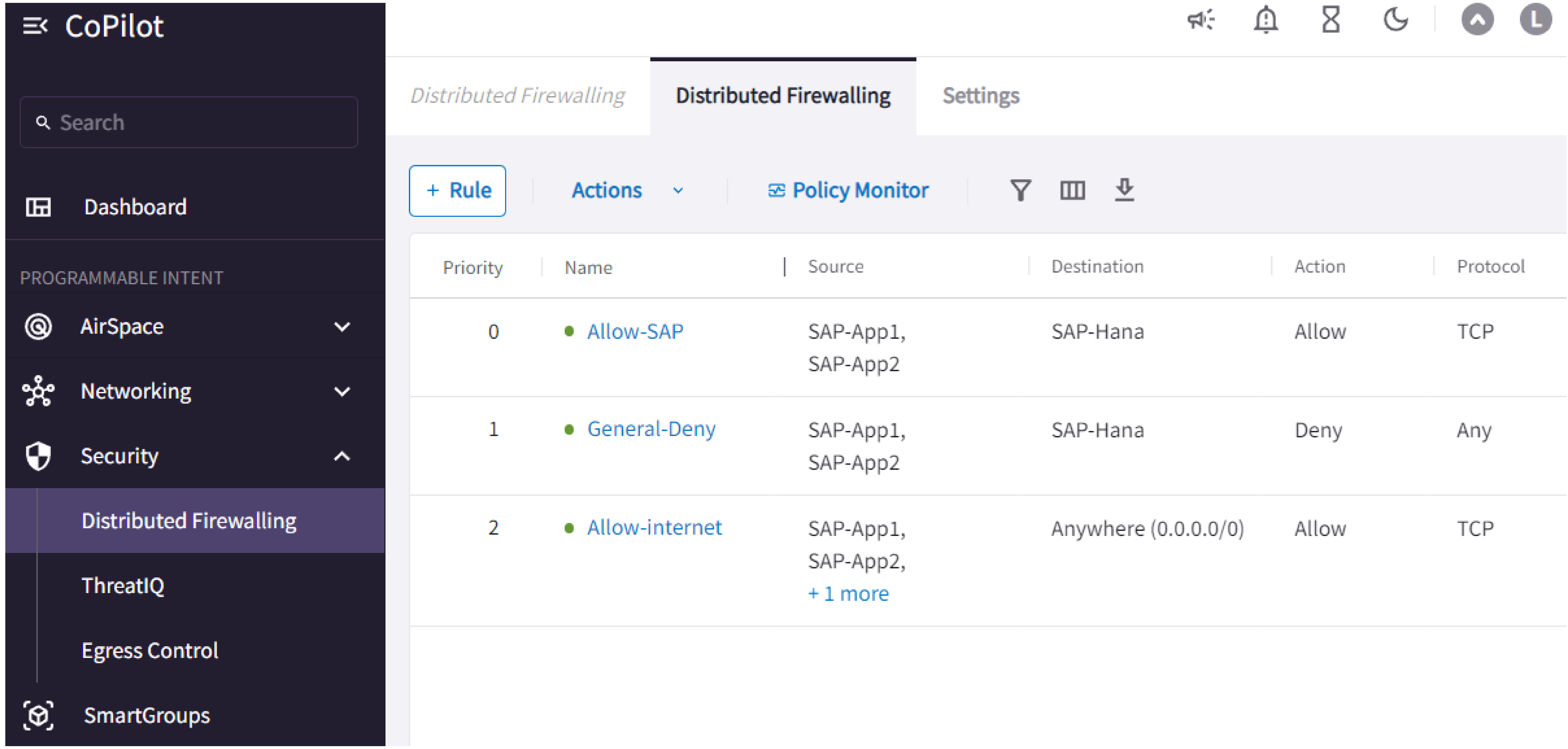
Priority	Name	Source	Destination	Action	Protocol
0	● Allow SAP	SAP-App1, SAP-App2	SAP-Hana	Allow	TCP
1	● General Deny	SAP-App1, SAP-App2	SAP-Hana	Deny	Any
2	● Allow internet	SAP-App1, SAP-App2, + 1 more	Anywhere (0.0.0.0/0)	Allow	TCP

You now have (3) firewall rules ready for Commit

Click **Commit** 1

Lab 5: Distributed Firewall: Step 5.5

Create Distributed Firewalling Rules



Priority	Name	Source	Destination	Action	Protocol
0	● Allow-SAP	SAP-App1, SAP-App2	SAP-Hana	Allow	TCP
1	● General-Deny	SAP-App1, SAP-App2	SAP-Hana	Deny	Any
2	● Allow-internet	SAP-App1, SAP-App2, + 1 more	Anywhere (0.0.0.0/0)	Allow	TCP

Our firewall rules have been deployed to the Aviatrix Spoke Gateways!

Let’s test them out…

Lab 5: Distributed Firewall: Step 5.5

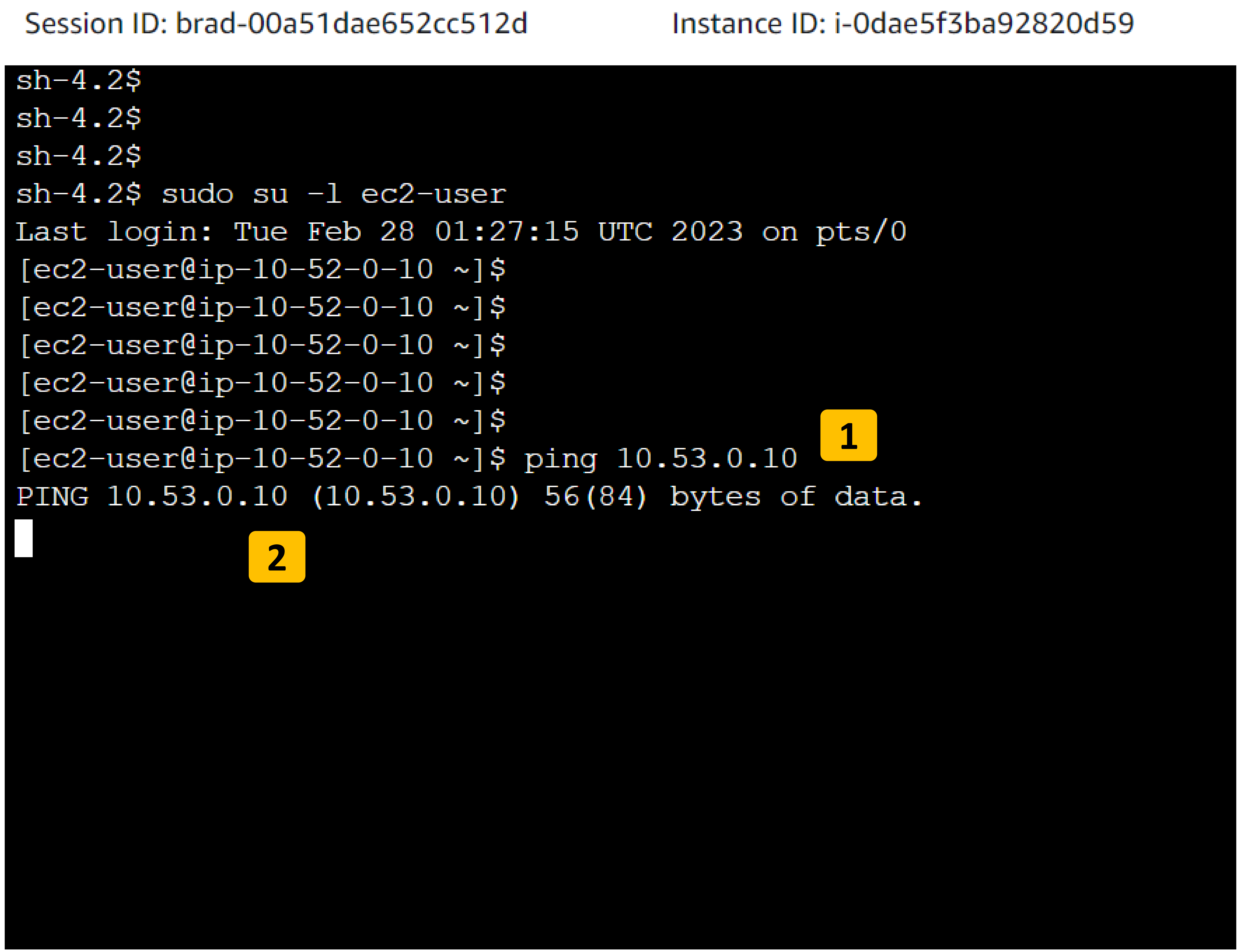
Test Distributed Firewalling Rules

Go the console of the EC2 instance **SAP2** in us-west-2

Try to ping SAP3 at **10.53.0.10** 1

This ping should **FAIL**, because our Distributed Firewall rules only allow TCP 8000 from the SAP1 and SAP2 instances to SAP3 2

Ctrl+C to exit the failing ping command



Session ID: brad-00a51dae652cc512d Instance ID: i-0dae5f3ba92820d59

```
sh-4.2$
sh-4.2$
sh-4.2$
sh-4.2$ sudo su -l ec2-user
Last login: Tue Feb 28 01:27:15 UTC 2023 on pts/0
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$ ping 10.53.0.10
PING 10.53.0.10 (10.53.0.10) 56(84) bytes of data.
```

Lab 5: Distributed Firewall: Step 5.5

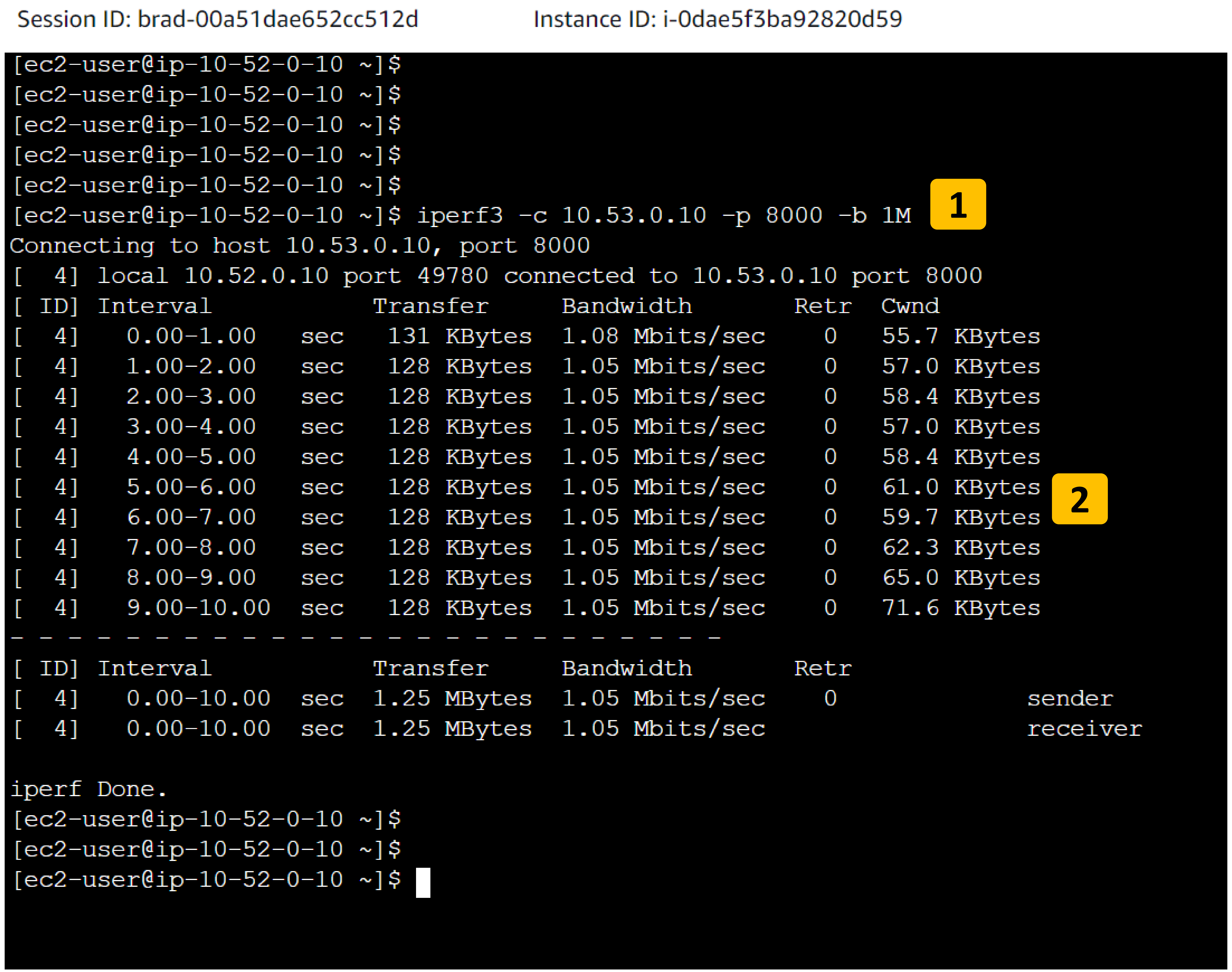
Test Distributed Firewalling Rules

At the console of the EC2 instance **SAP2**

Run the command:
iperf3 -c **10.53.0.10** -p 8000 –b 1M 1

This will open a TCP connection on port 8000 to SAP3 and transfer data.

This connection should **SUCCEED**, 2 because our Distributed Firewall rules allow TCP 8000 from the SAP1 and SAP2 instances to SAP3



Session ID: brad-00a51dae652cc512d Instance ID: i-0dae5f3ba92820d59

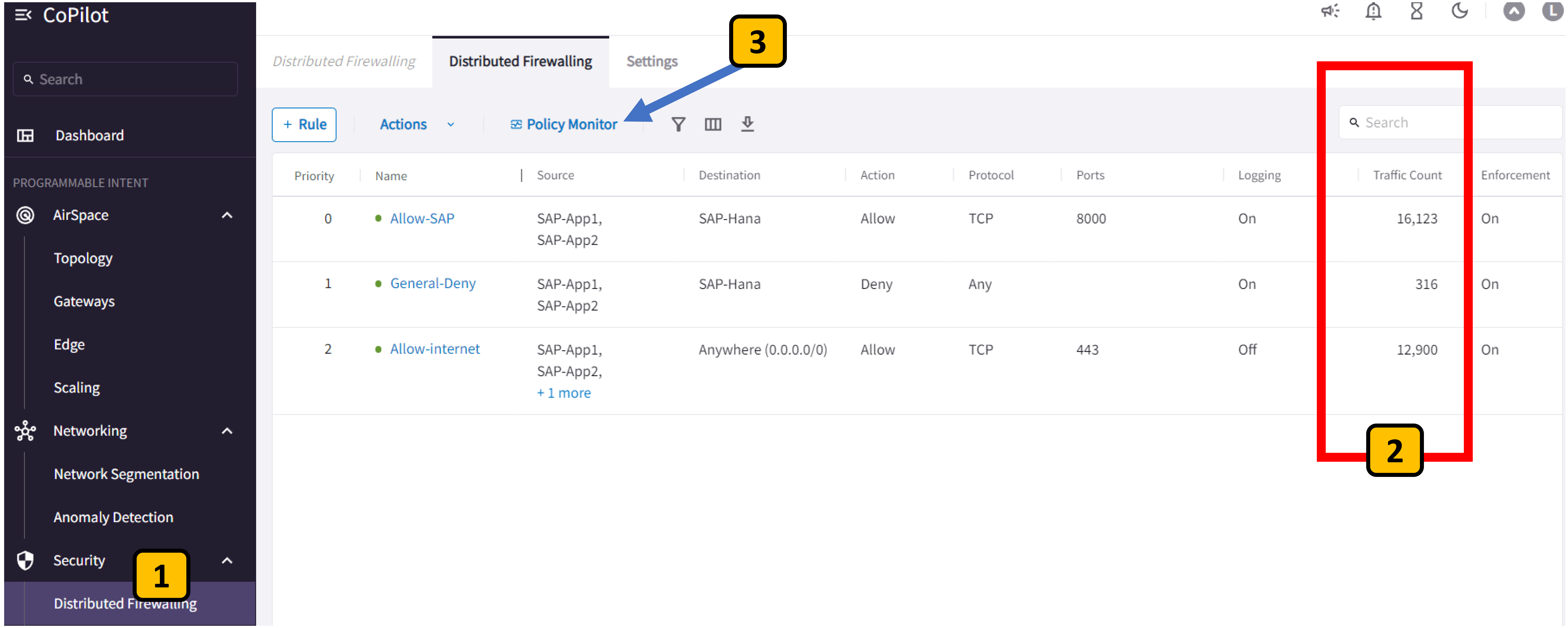
```
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$ iperf3 -c 10.53.0.10 -p 8000 -b 1M
Connecting to host 10.53.0.10, port 8000
[  4] local 10.52.0.10 port 49780 connected to 10.53.0.10 port 8000
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[  4]   0.00-1.00   sec   131 KBytes  1.08 Mbits/sec    0   55.7 KBytes
[  4]   1.00-2.00   sec   128 KBytes  1.05 Mbits/sec    0   57.0 KBytes
[  4]   2.00-3.00   sec   128 KBytes  1.05 Mbits/sec    0   58.4 KBytes
[  4]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec    0   57.0 KBytes
[  4]   4.00-5.00   sec   128 KBytes  1.05 Mbits/sec    0   58.4 KBytes
[  4]   5.00-6.00   sec   128 KBytes  1.05 Mbits/sec    0   61.0 KBytes
[  4]   6.00-7.00   sec   128 KBytes  1.05 Mbits/sec    0   59.7 KBytes
[  4]   7.00-8.00   sec   128 KBytes  1.05 Mbits/sec    0   62.3 KBytes
[  4]   8.00-9.00   sec   128 KBytes  1.05 Mbits/sec    0   65.0 KBytes
[  4]   9.00-10.00  sec   128 KBytes  1.05 Mbits/sec    0   71.6 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  4]   0.00-10.00  sec  1.25 MBytes  1.05 Mbits/sec    0             sender
[  4]   0.00-10.00  sec  1.25 MBytes  1.05 Mbits/sec                  receiver

iperf Done.
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
[ec2-user@ip-10-52-0-10 ~]$
```

aviatrix aws

Lab 5: Distributed Firewall: Step 5.5

Observe Distributed Firewall Traffic



Priority	Name	Source	Destination	Action	Protocol	Ports	Logging	Traffic Count	Enforcement
0	● Allow-SAP	SAP-App1, SAP-App2	SAP-Hana	Allow	TCP	8000	On	16,123	On
1	● General-Deny	SAP-App1, SAP-App2	SAP-Hana	Deny	Any		On	316	On
2	● Allow-internet	SAP-App1, SAP-App2, + 1 more	Anywhere (0.0.0.0/0)	Allow	TCP	443	Off	12,900	On

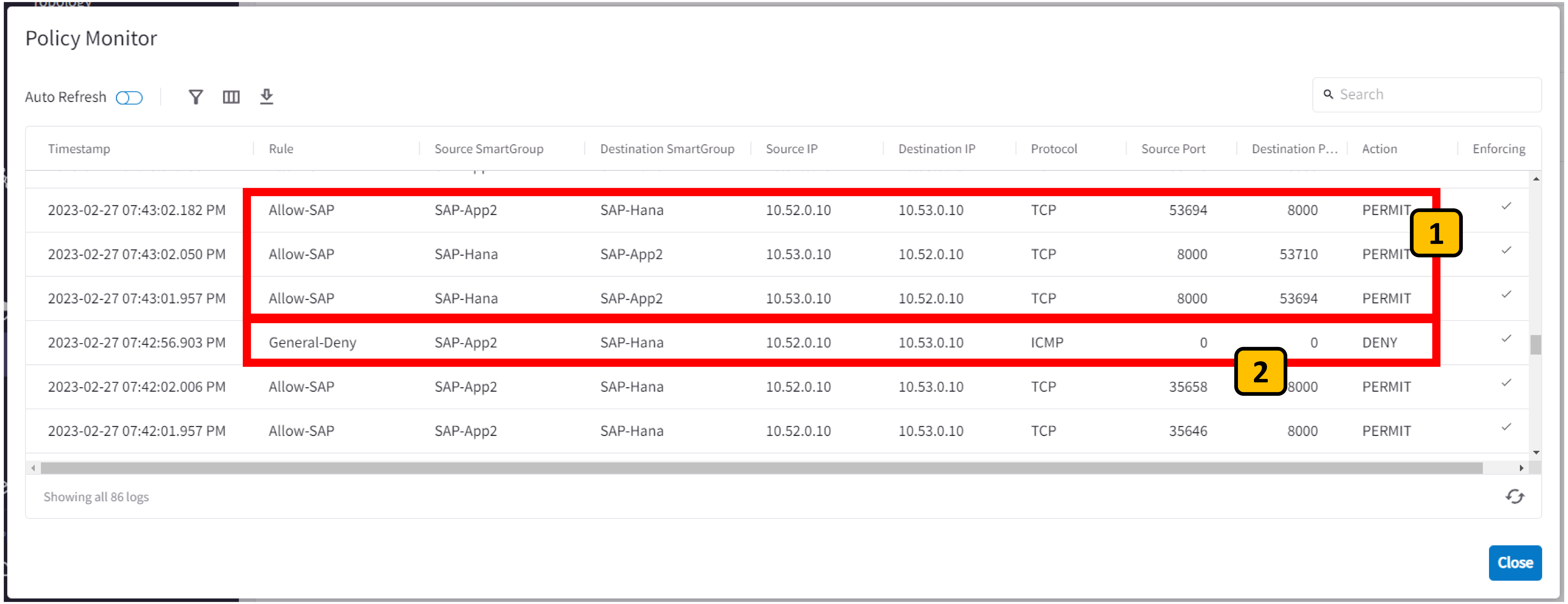
Go back Distributed Firewalling in CoPilot 1

Notice the Traffic Count for our rules 2

Click on Policy Monitor to see all the session details 3

Lab 5: Distributed Firewall: Step 5.5

Observe Distributed Firewall Traffic



Policy Monitor

Auto Refresh

Timestamp	Rule	Source SmartGroup	Destination SmartGroup	Source IP	Destination IP	Protocol	Source Port	Destination P...	Action	Enforcing
2023-02-27 07:43:02.182 PM	Allow-SAP	SAP-App2	SAP-Hana	10.52.0.10	10.53.0.10	TCP	53694	8000	PERMIT	✓
2023-02-27 07:43:02.050 PM	Allow-SAP	SAP-Hana	SAP-App2	10.53.0.10	10.52.0.10	TCP	8000	53710	PERMIT	✓
2023-02-27 07:43:01.957 PM	Allow-SAP	SAP-Hana	SAP-App2	10.53.0.10	10.52.0.10	TCP	8000	53694	PERMIT	✓
2023-02-27 07:42:56.903 PM	General-Deny	SAP-App2	SAP-Hana	10.52.0.10	10.53.0.10	ICMP	0	0	DENY	✓
2023-02-27 07:42:02.006 PM	Allow-SAP	SAP-App2	SAP-Hana	10.52.0.10	10.53.0.10	TCP	35658	8000	PERMIT	✓
2023-02-27 07:42:01.957 PM	Allow-SAP	SAP-App2	SAP-Hana	10.52.0.10	10.53.0.10	TCP	35646	8000	PERMIT	✓

Showing all 86 logs

In Policy Monitor you can see each TCP 8000 session that was Permitted 1

You can also see our ICMP Ping that was Denied 2

Lab 5 Intro

Distributed Firewall

PRODUCTION
SHARED
DEV
PCI
10.51.0.0/16
Spoke 1
Jump Instance
10.51.0.10
SAP1
10.52.0.0/16
Spoke 2
10.52.0.10
SAP2
10.52.0.0/16
Spoke 3
10.53.0.10
SAP3
10.0.0.0/16
VPC A
EC2-A
10.1.0.0/16
VPC B
EC2-B
Controller VPC
Aviatrix CoPilot
Aviatrix Controller
TCP 8000 ONLY
Transit
10.50.0.0/16
10.2.0.0/16
VPC C (Transit)
EC2-C
AWS us-west-2
AWS us-east-1

SUCCESS!! You completed Lab 5!

You're awesome.