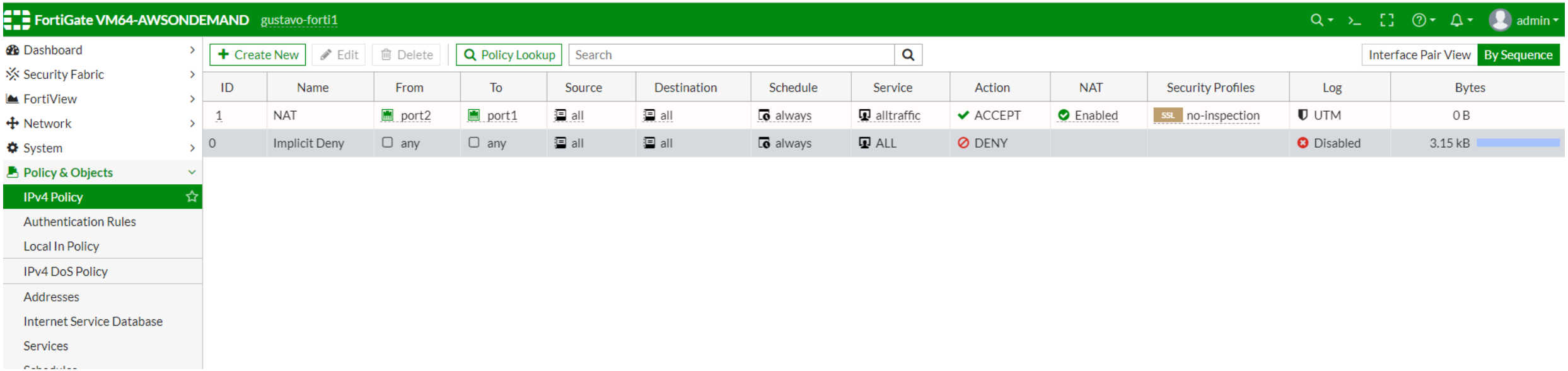
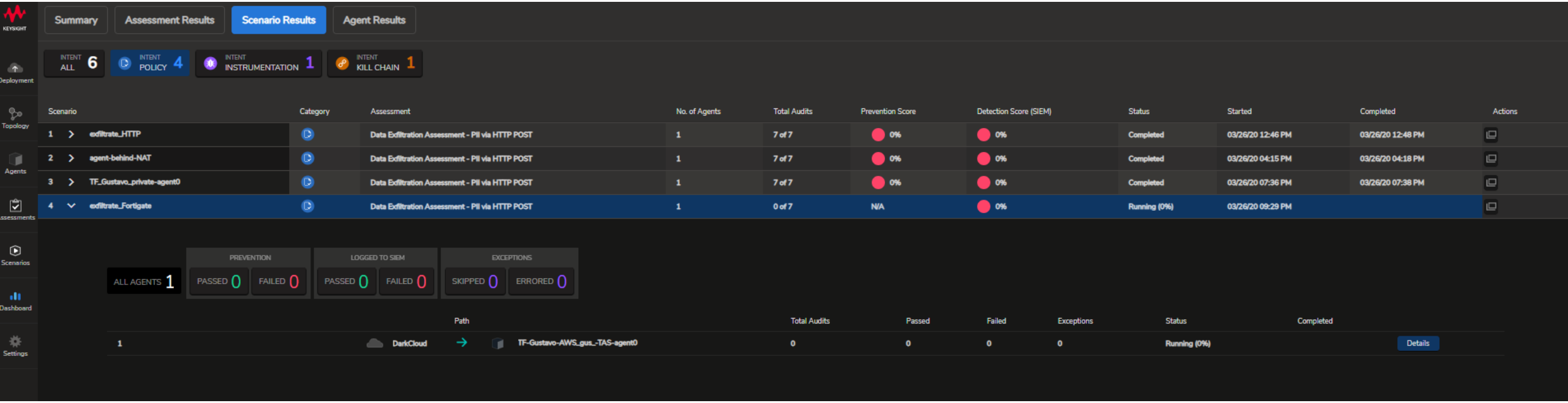
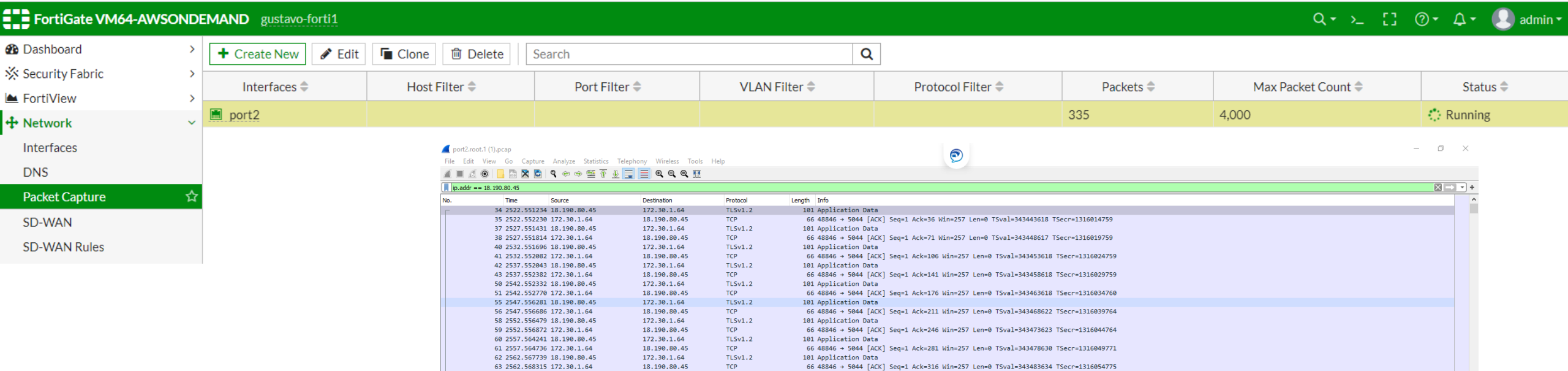
HOW TO CONFIGURE FORTIGATE VM

Declaring rule in Fortigate to allow outgoing traffic from agent towards Threat Attack simulator




Summary
Assessment Results
Scenario Results
Agent Results
INTENT ALL 6
INTENT POLICY 4
INTENT INSTRUMENTATION 1
INTENT KILL CHAIN 1
Scenario
Category
Assessment
No. of Agents
Total Audits
Prevention Score
Detection Score (SIEM)
Status
Started
Completed
Actions
1 exfiltrate_HTTP Data Exfiltration Assessment - PII via HTTP POST 1 7 of 7 0% 0% Completed 03/26/20 12:46 PM 03/26/20 12:48 PM
2 agent-behind-NAT Data Exfiltration Assessment - PII via HTTP POST 1 7 of 7 0% 0% Completed 03/26/20 04:15 PM 03/26/20 04:18 PM
3 TF_Gustavo_private-agent0 Data Exfiltration Assessment - PII via HTTP POST 1 7 of 7 0% 0% Completed 03/26/20 07:36 PM 03/26/20 07:38 PM
4 exfiltrate_Fortigate Data Exfiltration Assessment - PII via HTTP POST 1 0 of 7 N/A 0% Running (0%) 03/26/20 09:29 PM
ALL AGENTS 1
PREVENTION
PASSED 0
FAILED 0
LOGGED TO SIEM
PASSED 0
FAILED 0
EXCEPTIONS
SKIPPED 0
ERRORED 0
Path
Total Audits
Passed
Failed
Exceptions
Status
Completed
1 DarkCloud TF-Gustavo-AWS_gus_-TAS-agent0 0 0 0 0 Running (0%) Details


FortiGate VM64-AWSONDEMAND
gustavo-forti1
admin
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Create New
Edit
Clone
Delete
Search
Interfaces
Host Filter
Port Filter
VLAN Filter
Protocol Filter
Packets
Max Packet Count
Status
port2
335
4,000
Running
port2.root.1 (1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 18.190.80.45
No. Time Source Destination Protocol Length Info
34 2522.551234 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
35 2522.552230 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=36 Win=257 Len=0 TSval=343443618 TSecr=1316014759
37 2527.551431 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
38 2527.551814 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=71 Win=257 Len=0 TSval=343448617 TSecr=1316019759
40 2532.551696 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
41 2532.552082 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=106 Win=257 Len=0 TSval=343453618 TSecr=1316024759
42 2537.552043 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
43 2537.552382 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=141 Win=257 Len=0 TSval=343458618 TSecr=1316029759
50 2542.552332 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
51 2542.552770 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=176 Win=257 Len=0 TSval=343463618 TSecr=1316034760
55 2547.556281 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
56 2547.556686 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=211 Win=257 Len=0 TSval=343468622 TSecr=1316039764
58 2552.556479 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
59 2552.556872 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=246 Win=257 Len=0 TSval=343473623 TSecr=1316044764
60 2557.564241 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
61 2557.564736 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=281 Win=257 Len=0 TSval=343478630 TSecr=1316049771
62 2562.567739 18.190.80.45 172.30.1.64 TLSv1.2 101 Application Data
63 2562.568315 172.30.1.64 18.190.80.45 TCP 66 48846 → 5044 [ACK] Seq=1 Ack=316 Win=257 Len=0 TSval=343483634 TSecr=1316054775