

# FortiGate Firewall – Active Directory Integration via FSSO

## 1. Introduction

This document describes the complete setup and configuration of a FortiGate firewall (300D), integrated with Windows Server 2016 Active Directory (AD) using Fortinet Single Sign-On (FSSO). The project includes the deployment of VLANs, VDOMs, High Availability (HA), switch configuration, firewall policies, and user authentication testing.

---

## 2. Project Overview

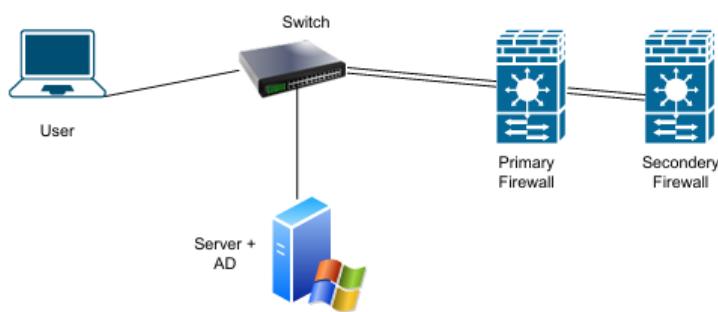
### Devices Used

- **FortiGate 300D** (2 units for HA)
- **Windows Server 2016** (Domain Controller + FSSO Agent)
- **Laptop (User PC)** connected to user VLAN
- **Switch** with VLANs for Server and User
- **Laptop for Management / Firewall Access**

### Purpose of the Project

- Integrate FortiGate with AD using FSSO
  - Enable user-based authentication for firewall policies
  - Learn configuration of VLANs, VDOMs, HA, and AD integration
  - Validate communication between VLANs
- 

## 3. Network Topology



Typical structure: - VLAN 10 – Users - VLAN 20 – Servers - Trunk link between Switch ↔ Firewall - FortiGate HA (Active-Passive or Active-Active)

---

## 4. Windows Server 2016 AD Configuration

### 4.0 Windows Server Installation Issues & Fixes

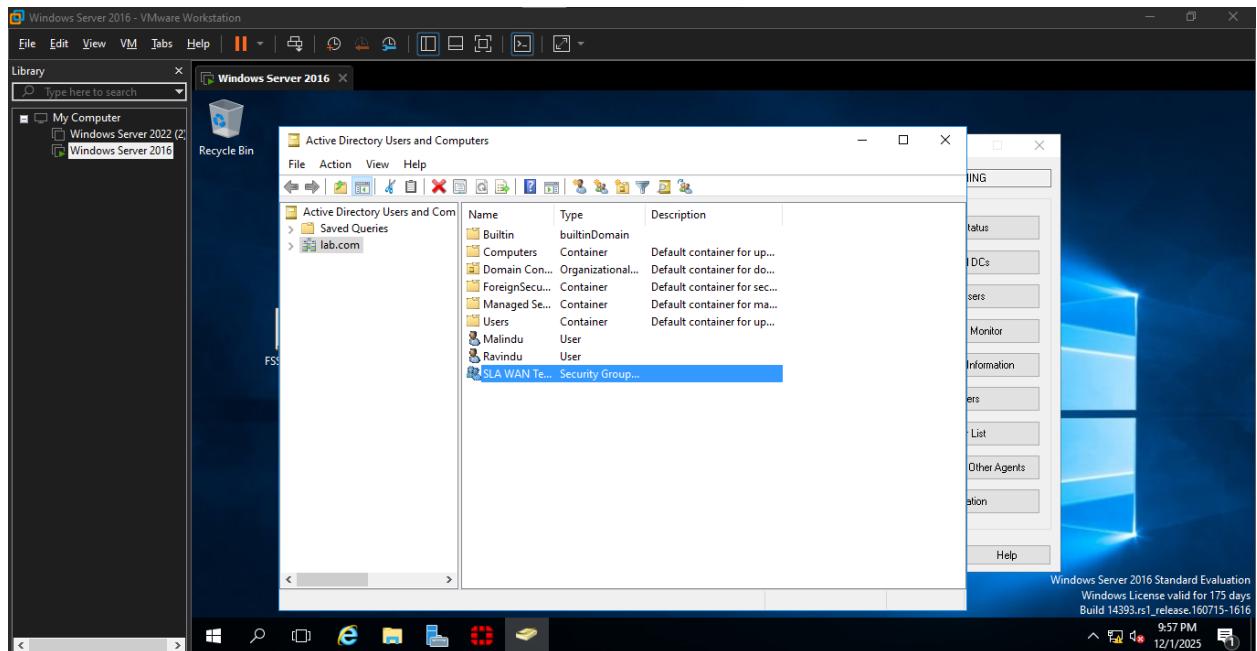
- **Error:** *Windows cannot find the Microsoft Software License Terms.*
  - **Fix:** Create VM **without ISO attached**, then add ISO afterward and boot.
- **Error:** *Timeout / EFI Network Boot (EFT Network)*
  - **Fix:** VM Settings → Options → Advanced → Switch BIOS/EFI mode → Restart installation.

### 4.1 Install Active Directory Domain Services

- Promote server to Domain Controller
- Create users via **AD Users and Computers**
  - Example user:
    - **ravindu** / Password: ####
- Promote server to Domain Controller
- Create domain users and groups

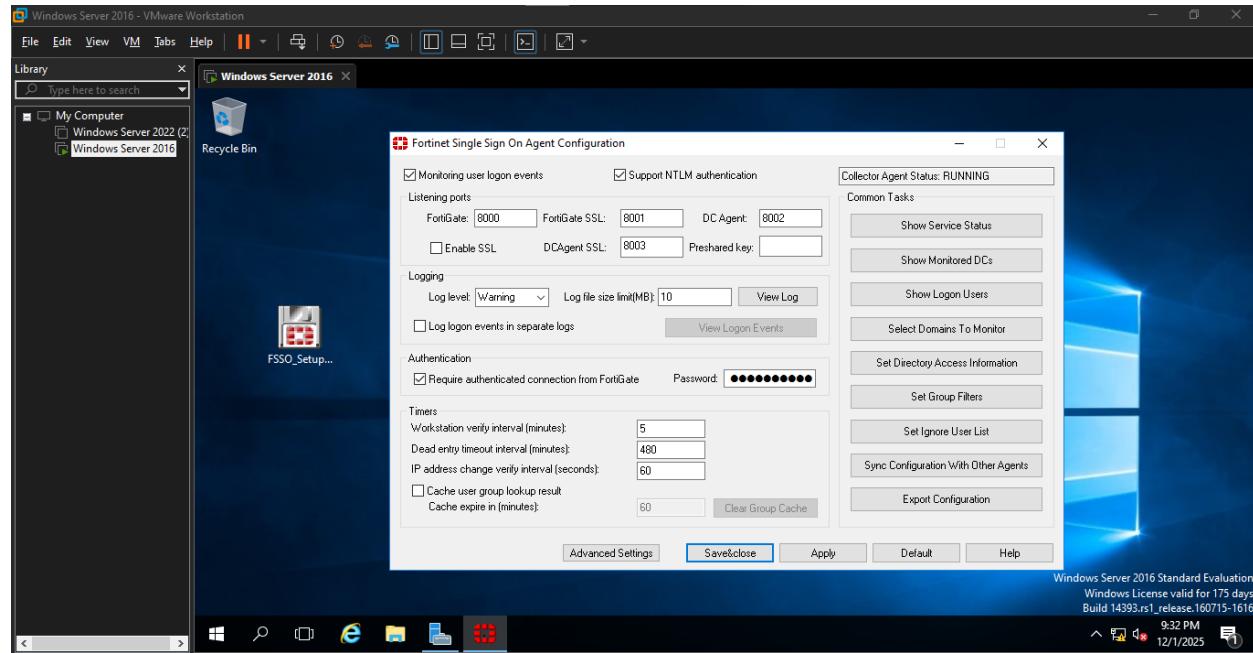
### 4.2 Setup DNS

- Ensure DNS entries for firewall and server
- Verify forward and reverse lookup zones



## 4.3 Install and Configure Fortinet FSSO Agent

Steps: 1. Install **FSSO Collector Agent** 2. Install **DC Agent** (optional if using polling mode)  
 3. Configure LDAP access credentials 4. Allow communication from Firewall to Collector  
 (TCP 8000/8002)



## 5. FortiGate Configuration

### 5.0 General Firewall Setup

- Create **VDOMs**
- Assign ports to VDOMs
- Enable **DHCP** on ports and set IP ranges
- Create **VLAN interfaces** for trunking (e.g., VLAN 10, VLAN 20)
- Create policy to allow access to **Domain Controller**

#### 5.1 Create VDOMs

- Example: root, user\_vdom, server\_vdom
- Assign interfaces to appropriate VDOMs

## 5.2 Configure Interfaces

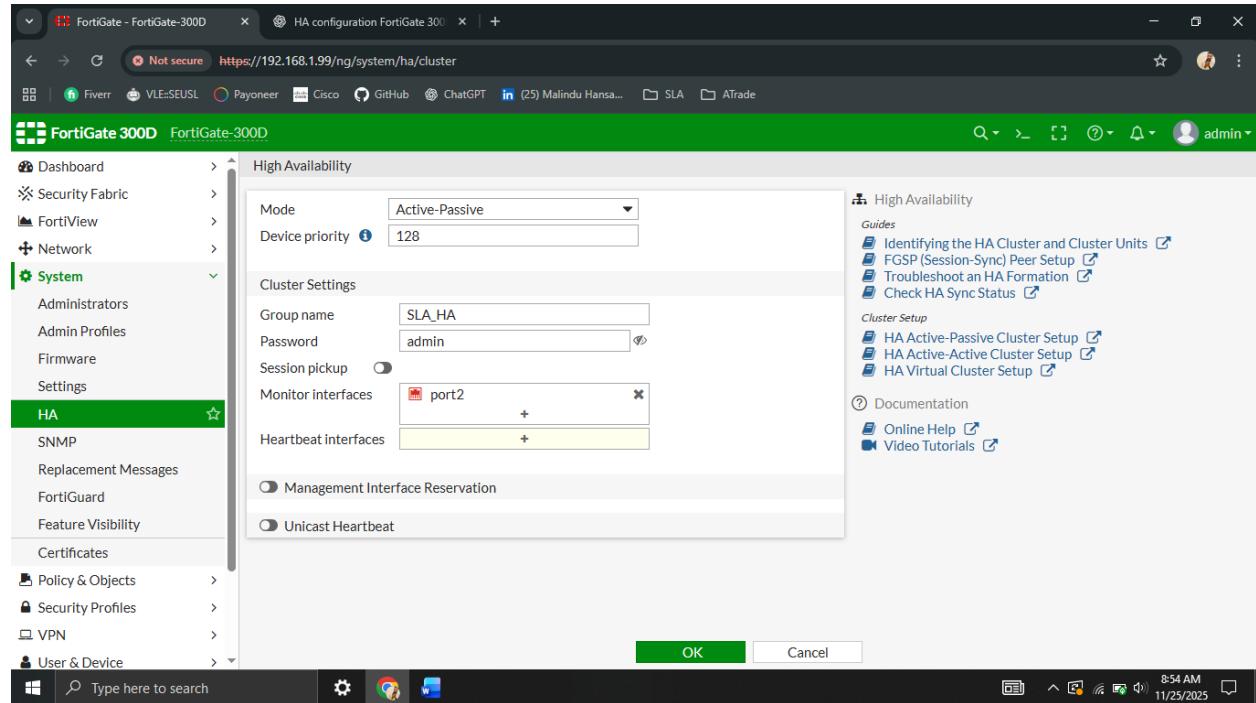
- Set VLAN sub-interfaces on the trunk port
- Example:
  - port2.10 for VLAN 10 (Users)
  - port2.20 for VLAN 20 (Servers)

## 5.3 Configure DHCP (optional)

- Enable DHCP server per VLAN

## 5.4 Configure HA Pair

Settings include: - Mode: Active-Passive - HBDEV: Heartbeat Interfaces - Sync: Sessions, Configurations



The screenshot shows the HA configuration page for a FortiGate 300D cluster. The left sidebar has a 'HA' section selected. The main area displays two FortiGate units in a table:

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
	128	FortiGate-300D	FGT3HD3915807177	Master	00:00:21:45	13	16.00 kbps
	64	FortiGate-300D	FGT3HD3916809471	Slave	00:00:09:02	12	25.00 kbps

The interface includes a toolbar at the top with 'Edit' and 'Remove device from HA cluster' buttons, and a bottom navigation bar with a search bar and system status indicators.

## 5.5 Firewall Policies

- Allow User VLAN → Internet
- Allow Server VLAN → Internet
- Inter-VLAN Rules if needed
- Policies referencing FSSO user groups

## 6. FSSO Authentication Setup on FortiGate

### 6.0 FSSO Installation on Server

- Download and install FSSO
- Set password: **Airbus@330**
- Turn off Windows Firewall during installation

### 6.1 Configure FSSO Connector on FortiGate

- Go to **Security Fabric > External Connectors**
- Create new FSSO connector
- Enter server IP + FSSO password
- Test connectivity #### 6.1 Add LDAP Server
- Base DN, Bind DN, Authentication type

The screenshot shows the FortiGate 300D web interface. The left sidebar is titled "External Connectors" and includes options like Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report. The main content area is titled "FSSO Agent on Windows AD" and shows a list of 50 FSSO connectors.

## 6.2 Add FSSO Connector

- IP of Collector Agent
- Port 8000/8002
- Test connectivity

## 6.3 Create User Groups

- Map AD Groups with FSSO Groups

The screenshot shows the "Edit External Connector" page for the "FSSO Agent on Windows AD" connector. The left sidebar is identical to the previous screenshot. The main content area is titled "Collector Agent Group Filters" and shows a table mapping AD Groups to User Groups. The "LAB/SLA WAN TEAM" group is highlighted in yellow.

AD Group	User Groups	Ref.
LAB/RDS MANAGEMENT SERVERS		
LAB/RDS REMOTE ACCESS SERVERS		
LAB/READ-ONLY DOMAIN CONTROLLERS		
LAB/REMOTE DESKTOP USERS		
LAB/REMOTE MANAGEMENT USERS		
LAB/REPLICATOR		
LAB/SCHEMA ADMINS		
LAB/SERVER OPERATORS		
LAB/SLA WAN TEAM		
LAB/STORAGE REPLICA ADMINISTRATORS		
LAB/SYSTEM MANAGED ACCOUNTS GROUP		
LAB/TERMINAL SERVER LICENSE SERVERS		
LAB/USERS		
LAB/WINDOWS AUTHORIZATION ACCESS GROUP		

## 6.4 Apply User-Based Firewall Policies

- Example: Allow Only AD Users in group Employees to access internet
- 

## 7. Switch Configuration

- Create VLANs 10 and 20
  - Assign access ports for server and user devices
  - Configure trunk port to FortiGate
- 

## 8. Testing & Verification

### 8.1 Ping Connectivity

- User VLAN → Server VLAN
- User VLAN → Gateway
- Firewall ↔ Server communication

### 8.2 Authentication Testing

- Log in with domain account from user laptop
- Verify FSSO user detected in FortiGate → User & Device > Monitor
- Check traffic logs

### 8.3 Failover Testing (HA)

- Disconnect primary firewall
  - Ensure secondary takes over
- 

## 9. Conclusion

This project demonstrates the full workflow of integrating FortiGate firewall with Windows AD using FSSO, complete VLAN separation, HA failover, VDOM usage, and authentication-based policy enforcement.

---

## 11. References

- Fortinet Documentation and Cookbooks
- Windows Server 2016 AD Guidelines