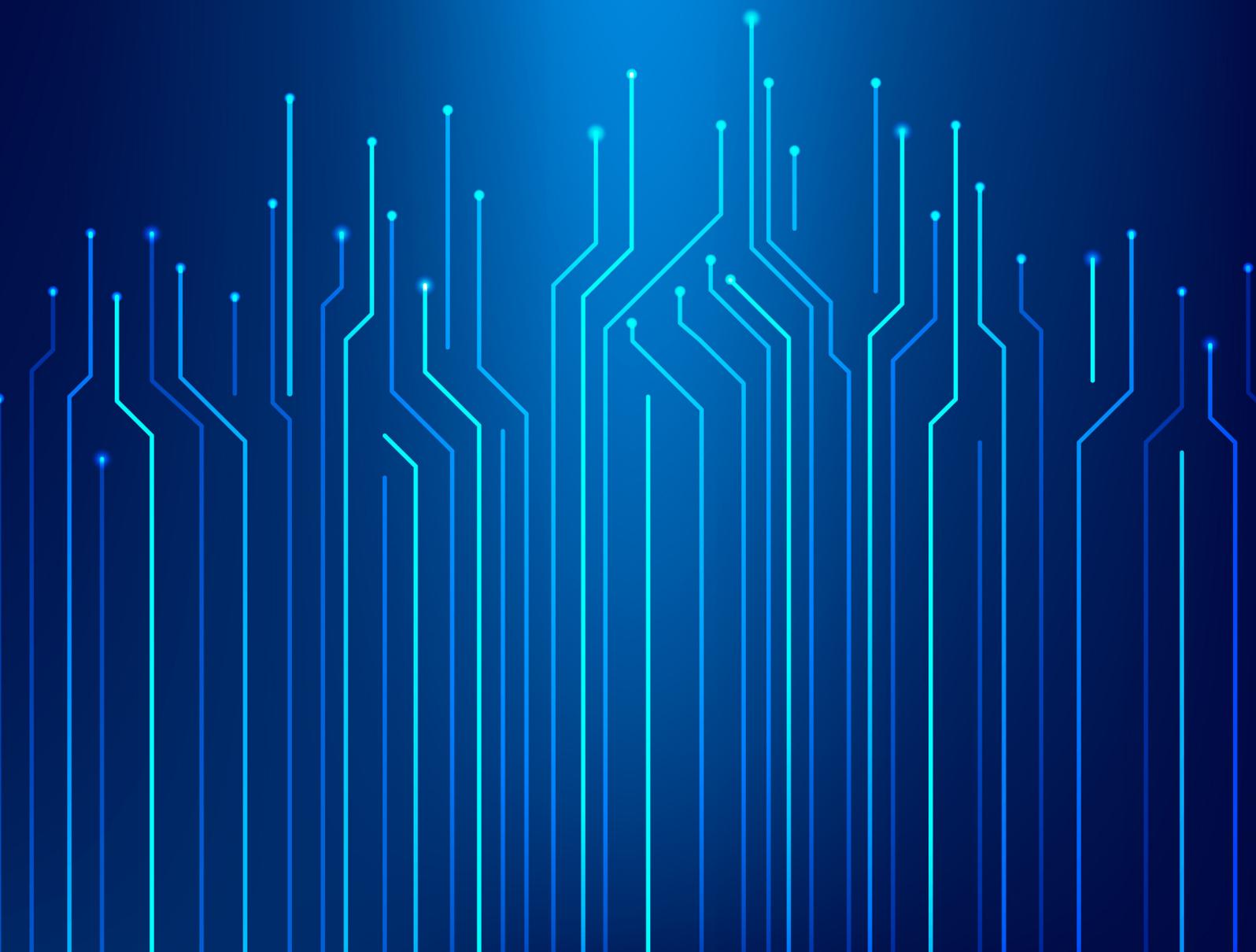


How to configure AD on your firewall



How to configure AD on your firewall

Active Directory is Microsoft's trademarked directory service, an integral part of the Windows architecture. Active Directory is a centralized and standardized system that automates network management of user data, security, and resources.

Step 1: Create a service group on the firewall by going to Definitions -> Protocols and Services -> Configure Service Group.

Configure Service Group	
Group	AD
Available Services	Selected Services
microsoft-sql_monitortcp microsoft-sql_monitorudp microsoft-sql_servertcp microsoft-sql_serverudp MSN news nntp ntp oracle oracle_sql_net	microsoft-smbtcp netbios-dgmtcp netbios-dgmudp netbios-nstcp netbios-ssntcp netbios-ssnudp
<input type="button" value="Add"/>	

Step 2: Create a host by going to Definitions-> Hosts and add ADServer as a host by specifying the appropriate IP Address.

Add Host	
Host ID	ADServer
Host IP	192.168.2.242
<input type="button" value="Add"/>	

Step 3: Now create the rules for allowing AD service through the GajShield firewall by going to Firewall -> Policies -> Rules

You will need to add a rule by going on Firewall -> Policies -> Rules & use ADServer in services tab, to allow the firewall to access the Active Directory Server as shown below.

Zones			
Direction	Any	To	Any
Source	fwip-LAN	NAT	Ignore
Destination	ADServer	NAT	No NAT

Services and Ports			
Services	AD	NAT	No NAT

NOTE: After adding the firewall rules, install the firewall policies by going to Firewall -> Policies -> Install Policies

Step 3: Now go to Configuration -> User Management -> Active Directory and configure AD as shown below.

Add Active Directory Settings	
Workgroup Name	testdc
Server Name	activedirectory-server
Domain Name	testdc.com
Server IP	AD-Server
Username	administrator
Password
Enable Group Synchronization	<input type="checkbox"/>
<input type="button" value="Add"/>	

Workgroup name: Type you domain name without abbreviation. (Example: Domain name is testdc.com, only insert testdc).

Server name: Insert the host name / NetBIOS name of the server.

Domain name: Insert Domain name. (Example: Domain name is testdc.com, insert the same).

Server IP: Select the Domain controller LAN IP Host.

Username: Provide username of an administrator or any user with administrative right. (Recommended is administrator user).

Password: Insert password of the user in the Username field.

Enable Group Synchronization: Check if you want to enable user group synchronization from active directory.

Join Active Directory Domain



Join Active Directory Domain: After adding active directory settings, click on Join button to join active directory domain server.

Synchronize Active Directory Users



Synchronize Active Directory Users: After joining the active directory domain server, click on Synchronize button to synchronize active directory domain server users and groups.

NOTE: You will have to specify Active Directory option by going to Browsing -> Setup -> Browsing Options, tick on userSense and specify Active Directory from the drop down menu.

Browsing Setup		
URL Blocker Instance	10	
Enforce Strict Search on	<input checked="" type="checkbox"/> Google Images <input type="checkbox"/> Yahoo Images	
Enable Virus Scanning	<input checked="" type="checkbox"/>	
Large File Download Alert Limit	1024 KB (0 Means no alerts generated)	
App Filter Policy	Please Select ▼	
URL Filter Policy	Open ▼	
URL Filter QoS	TestPolicy ▼	

Browsing Mode Configuration		
Browsing Mode	SSL Deep Inspect	Authentication
<input checked="" type="checkbox"/> Proxy Mode Proxy Port: 3128	<input checked="" type="checkbox"/>	<input type="radio"/> No Authentication <input type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> TACACS+ <input type="radio"/> LDAP <input checked="" type="radio"/> Active Directory
<input checked="" type="checkbox"/> Gateway Mode	<input checked="" type="checkbox"/>	<input type="radio"/> No Authentication <input checked="" type="radio"/> GajShield userSense Choose your preference: 1. Active Directory ▼ 2. Local ▼ 3. Please Select ▼ Enable Single Sign On: Yes ▼ Select logout time interval (in minutes): 1 ▼

Setup

NOTE: Active Directory domain groups will only synchronize if "Enable Group Synchronization" is selected under Active Directory Settings.

Thus, you have configured AD on your firewall.