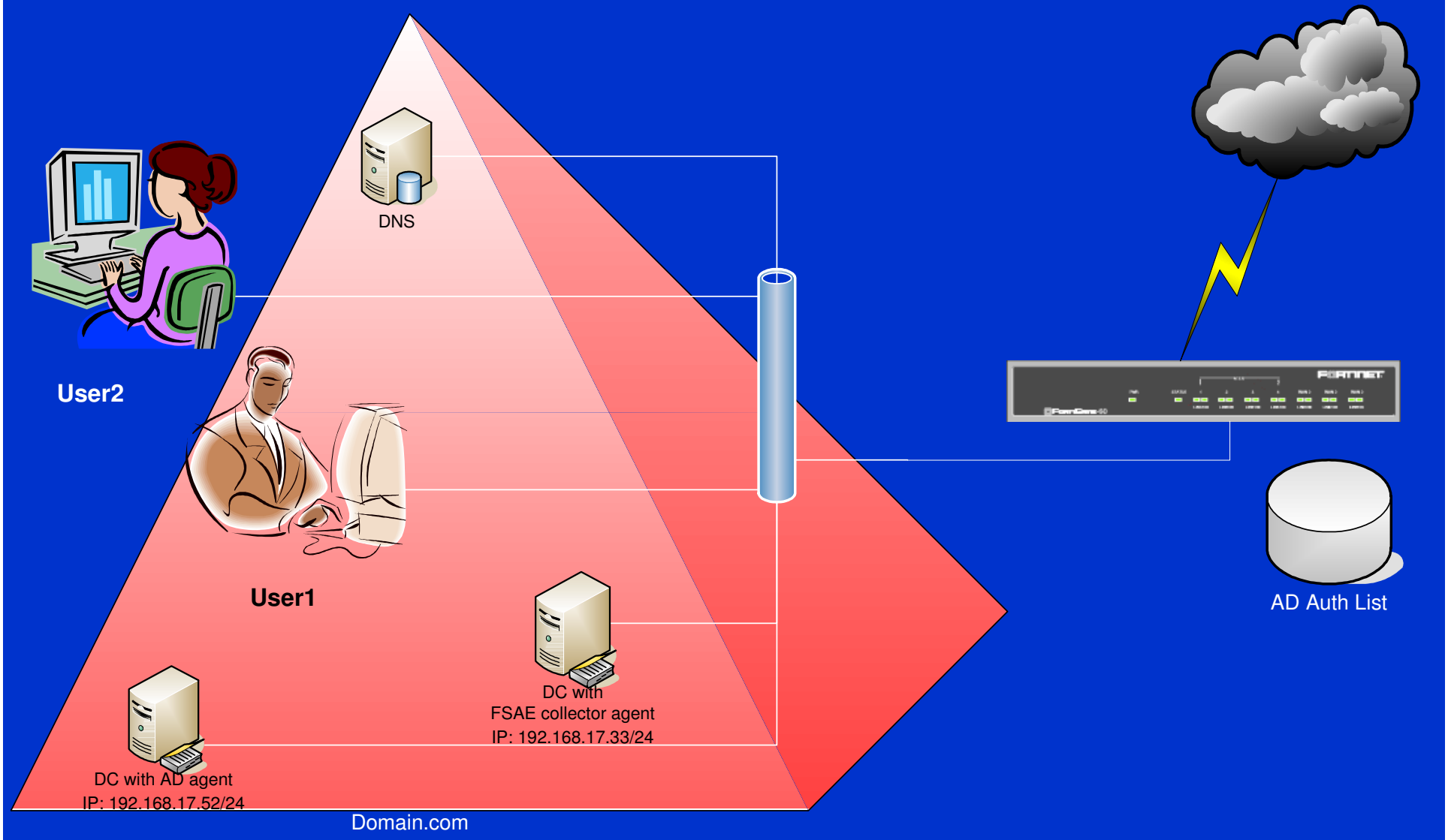
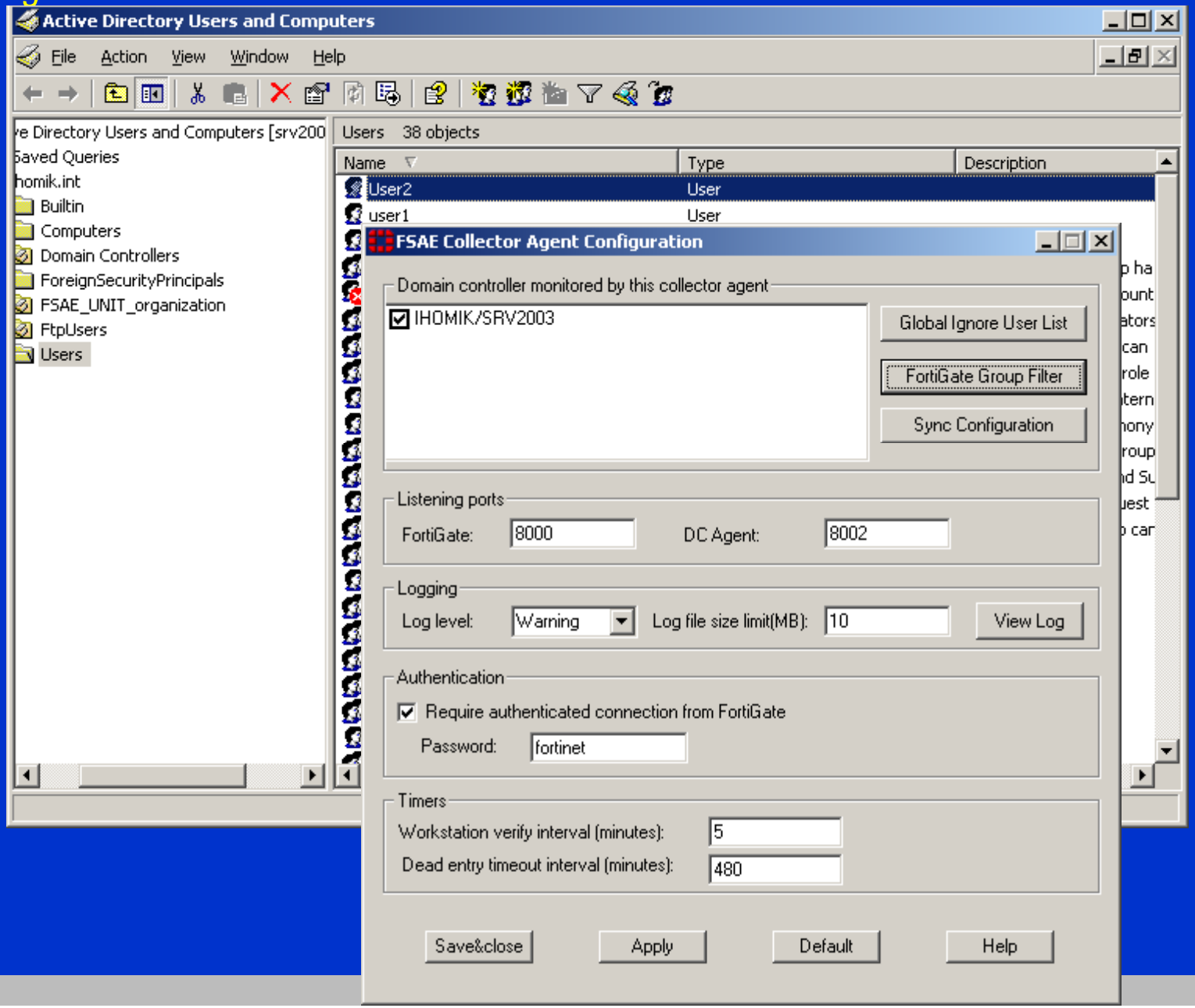
FSAE for FortiOS v3.0

FORTINET

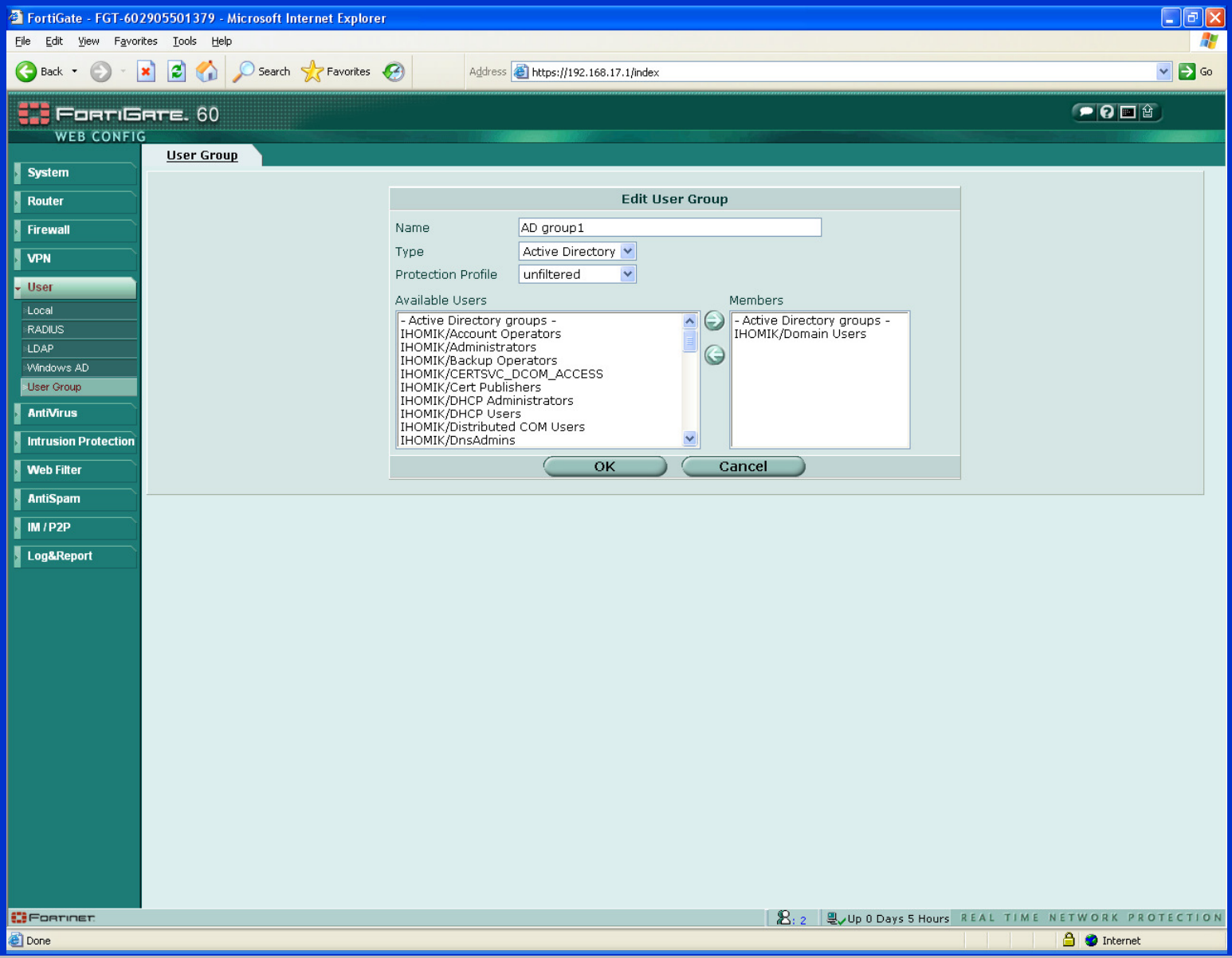
What it is for?



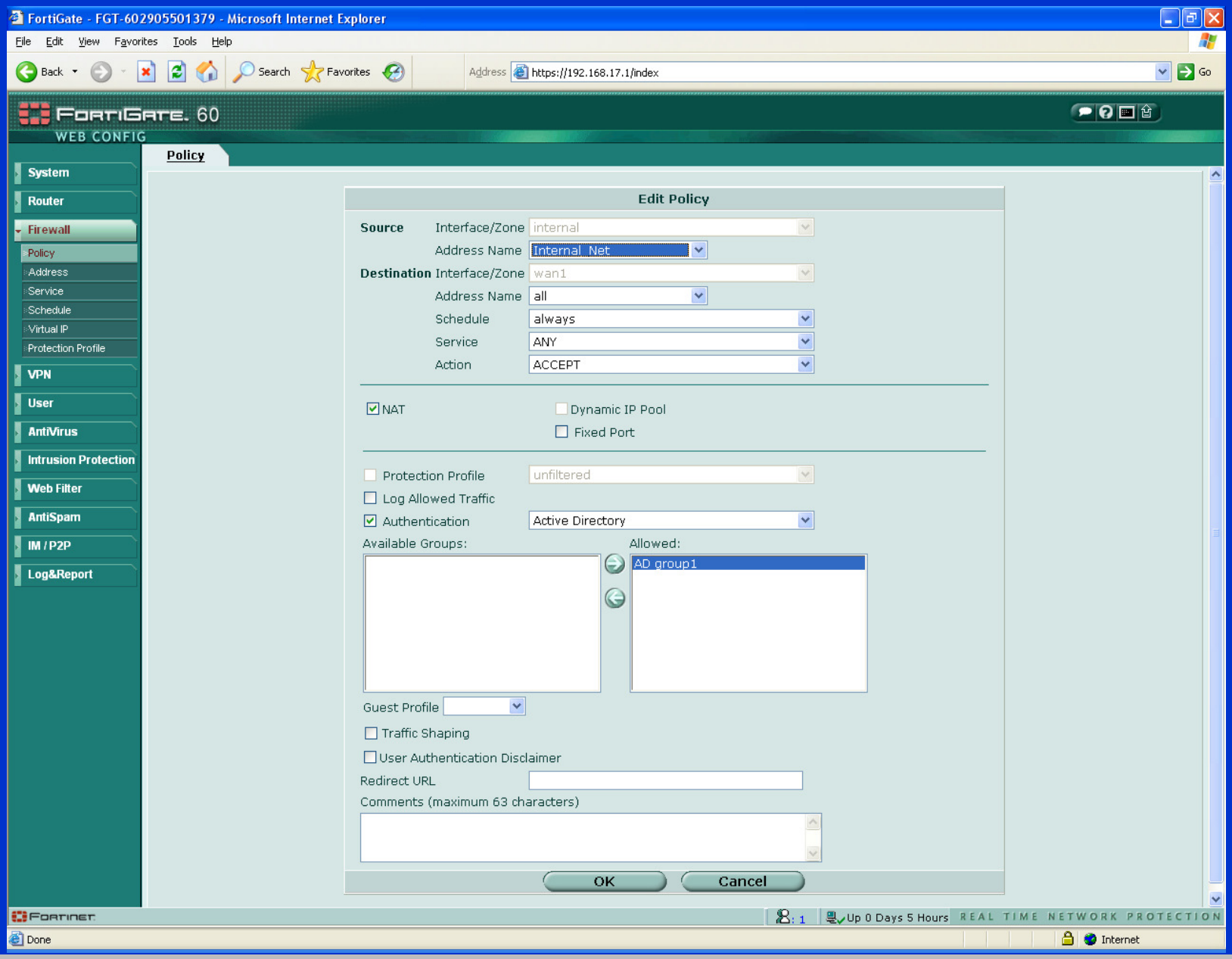
Configuring



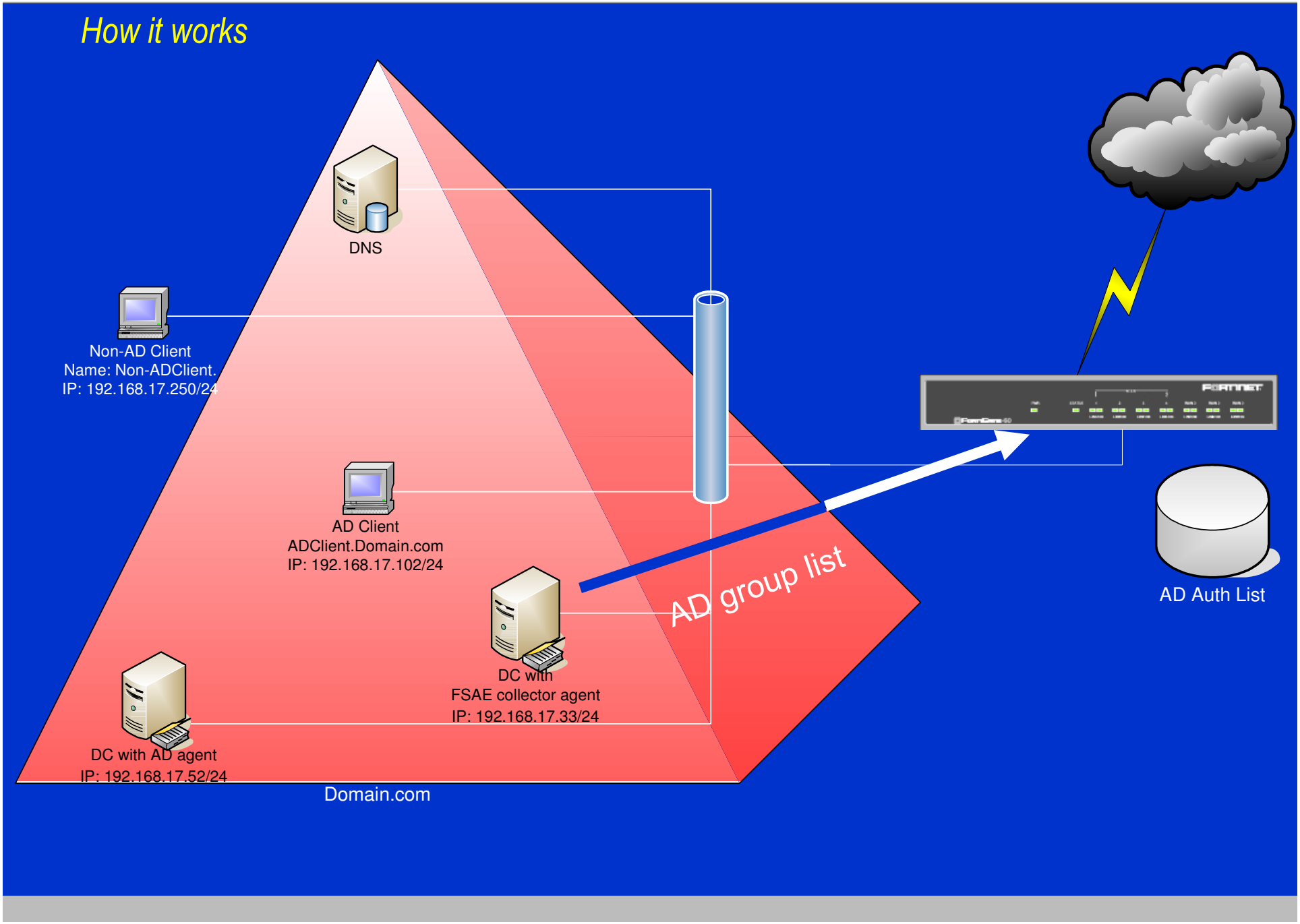
Configuring



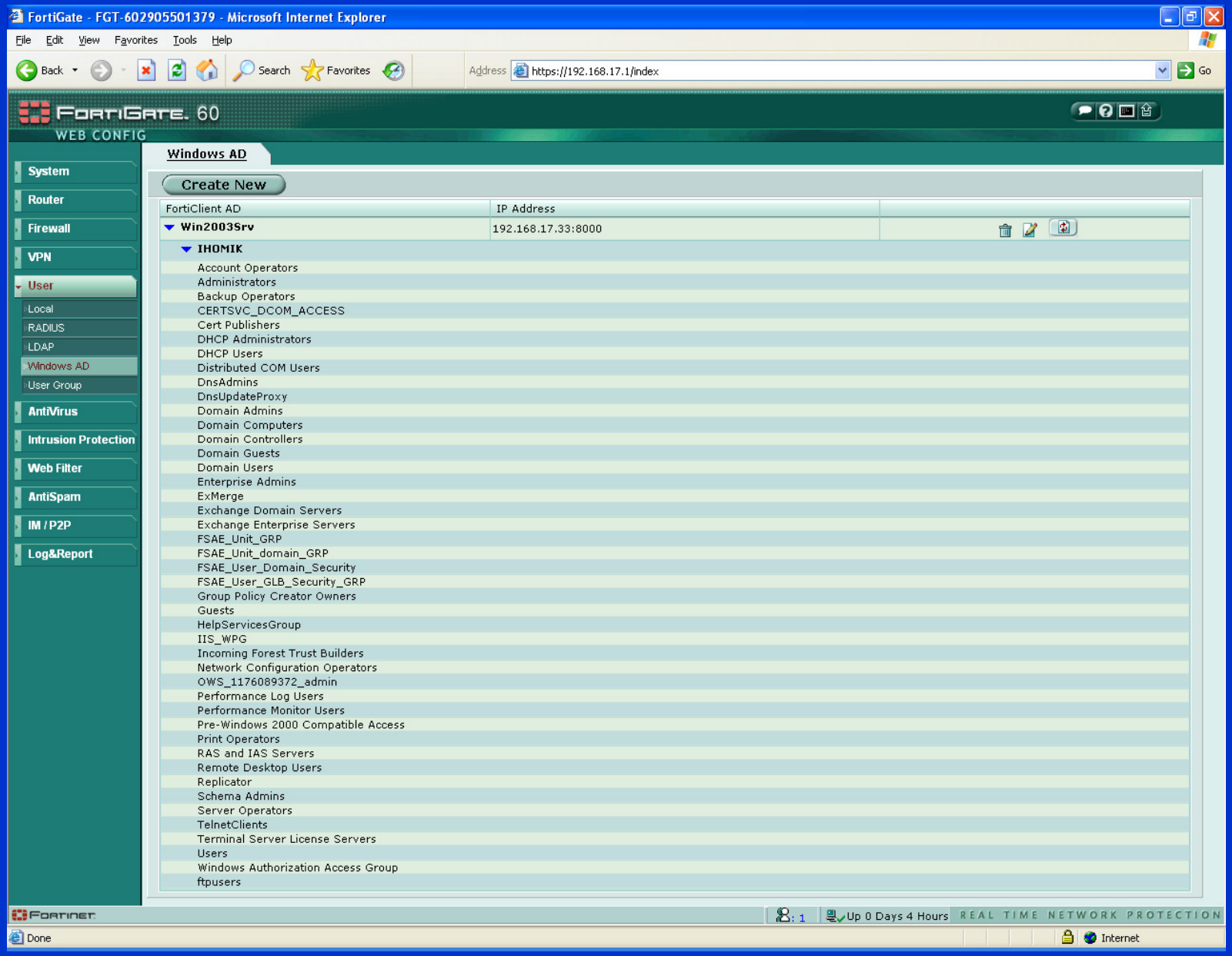
Configuring



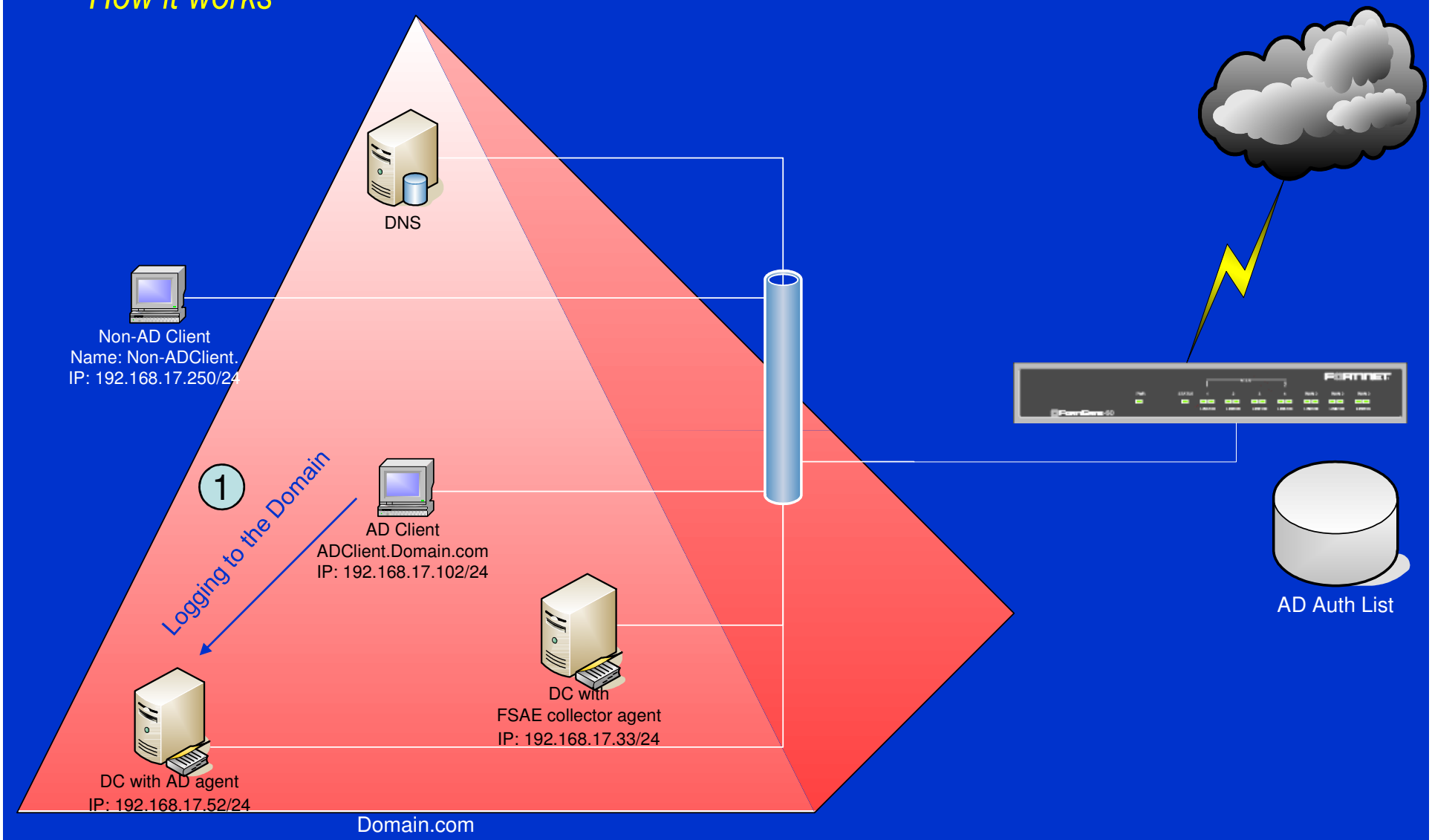
How it works


DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
AD group list
AD Auth List

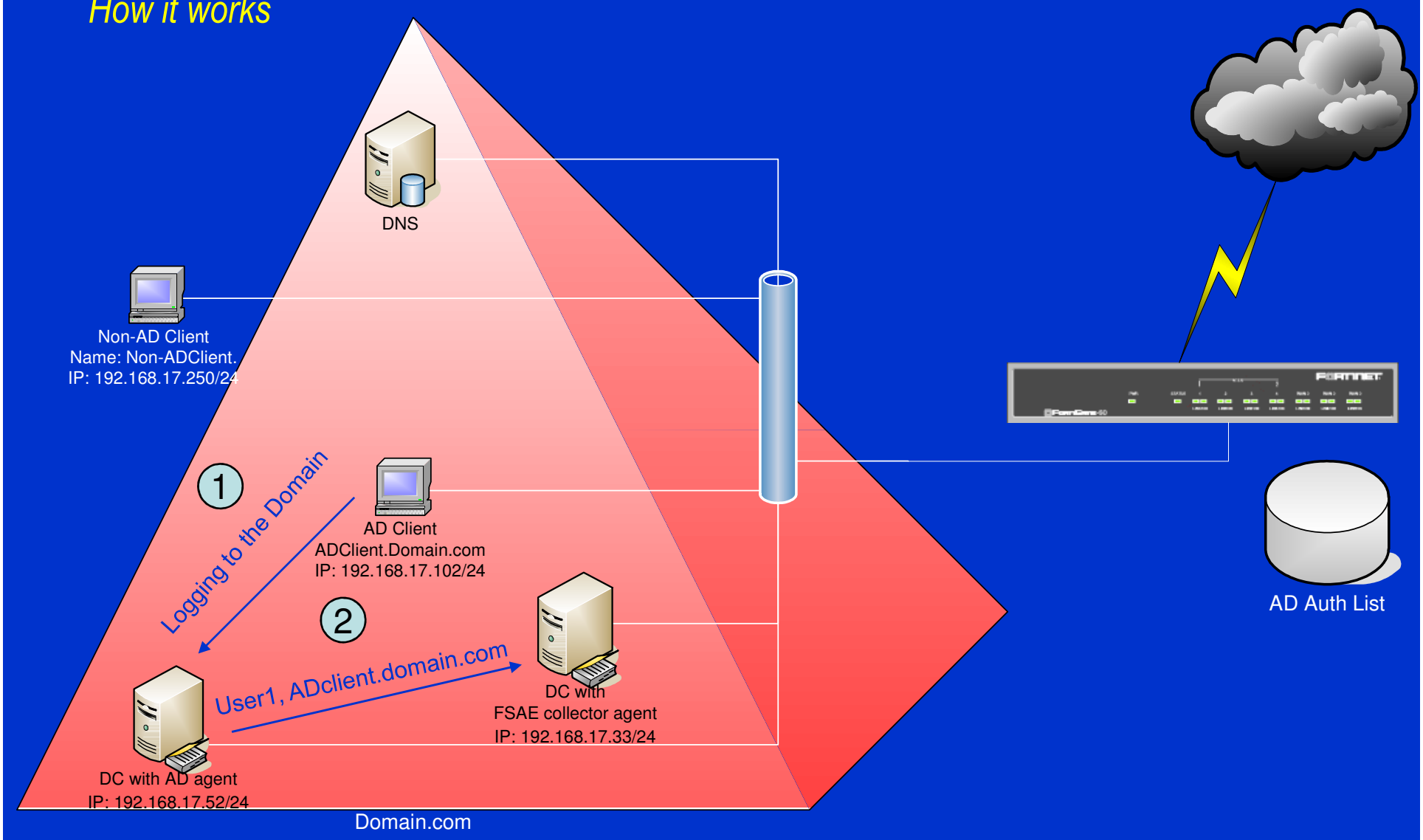
How it works


FortiGate - FGT-602905501379 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.17.1/index
Go
FortiGate 60
WEB CONFIG
System
Router
Firewall
VPN
User
Local
RADIUS
LDAP
Windows AD
User Group
AntiVirus
Intrusion Protection
Web Filter
AntiSpam
IM / P2P
Log&Report
Windows AD
Create New
FortiClient AD
IP Address
Win2003Srv
192.168.17.33:8000
IHOMIK
Account Operators
Administrators
Backup Operators
CERTSVC_DCOM_ACCESS
Cert Publishers
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
ExMerge
Exchange Domain Servers
Exchange Enterprise Servers
FSAE_Unit_GRP
FSAE_Unit_domain_GRP
FSAE_User_Domain_Security
FSAE_User_GLB_Security_GRP
Group Policy Creator Owners
Guests
HelpServicesGroup
IIS_WPG
Incoming Forest Trust Builders
Network Configuration Operators
OWS_1176089372_admin
Performance Log Users
Performance Monitor Users
Pre-Windows 2000 Compatible Access
Print Operators
RAS and IAS Servers
Remote Desktop Users
Replicator
Schema Admins
Server Operators
TelnetClients
Terminal Server License Servers
Users
Windows Authorization Access Group
ftpusers
Fortinet
1
Up 0 Days 4 Hours
REAL TIME NETWORK PROTECTION
Done
Internet

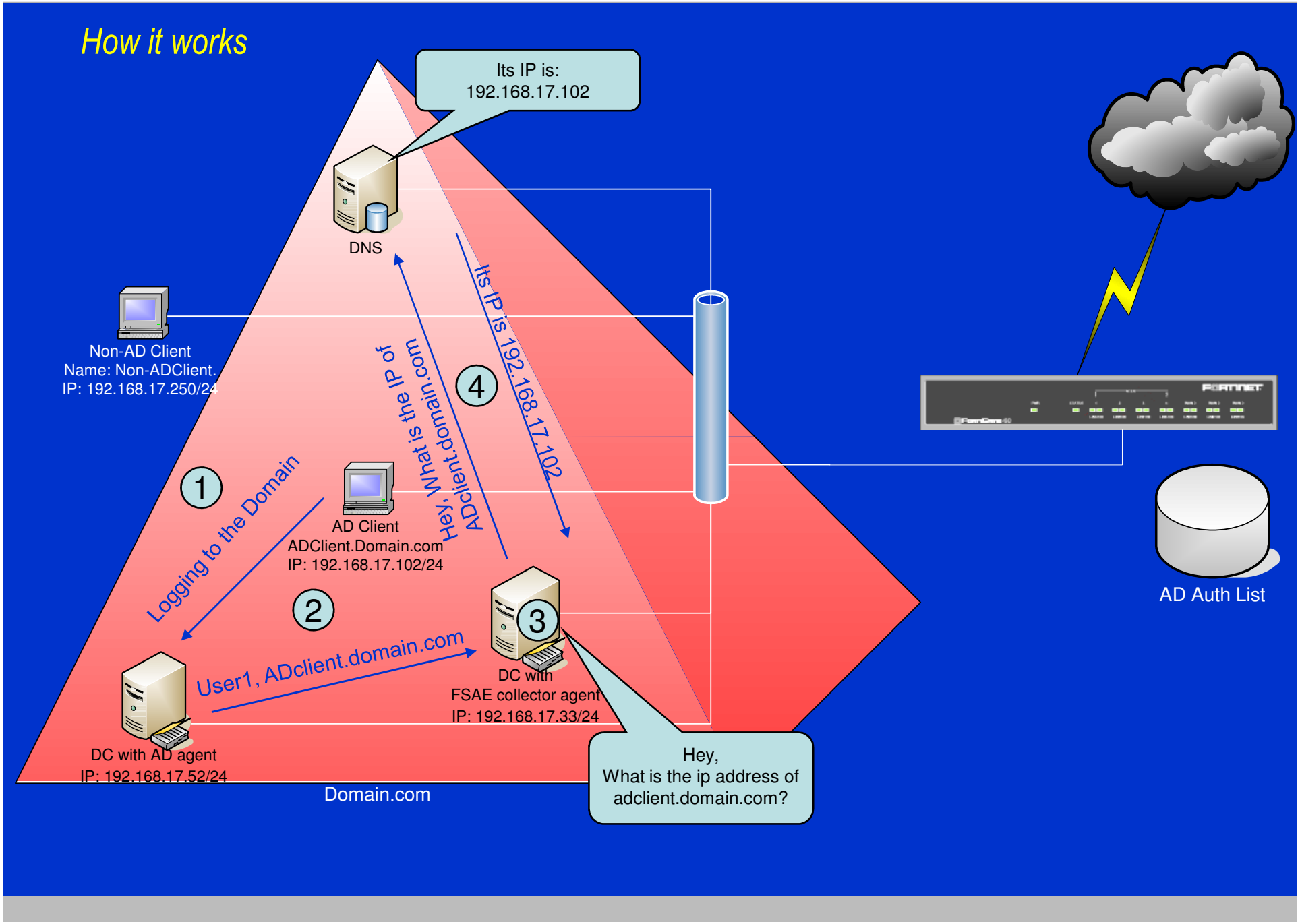
How it works


DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
1
Logging to the Domain
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
AD Auth List

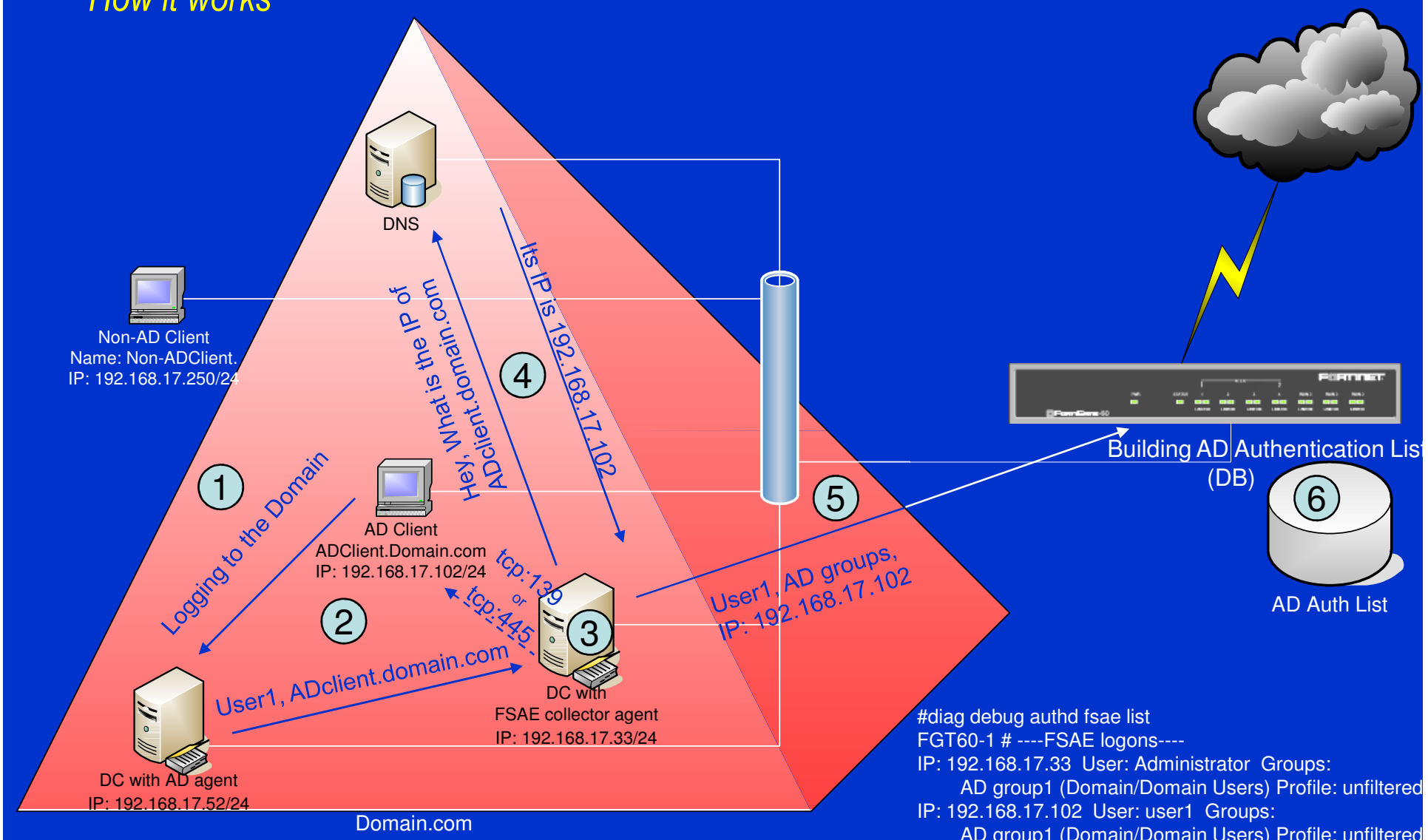
How it works


DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
1
Logging to the Domain
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
2
User1, ADclient.domain.com
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
AD Auth List

How it works


Its IP is:
192.168.17.102
DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
Logging to the Domain
1
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
Hey, What is the IP of ADclient.domain.com
4
Its IP is 192.168.17.102
2
User1, ADclient.domain.com
3
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
Hey,
What is the ip address of
adclient.domain.com?
AD Auth List

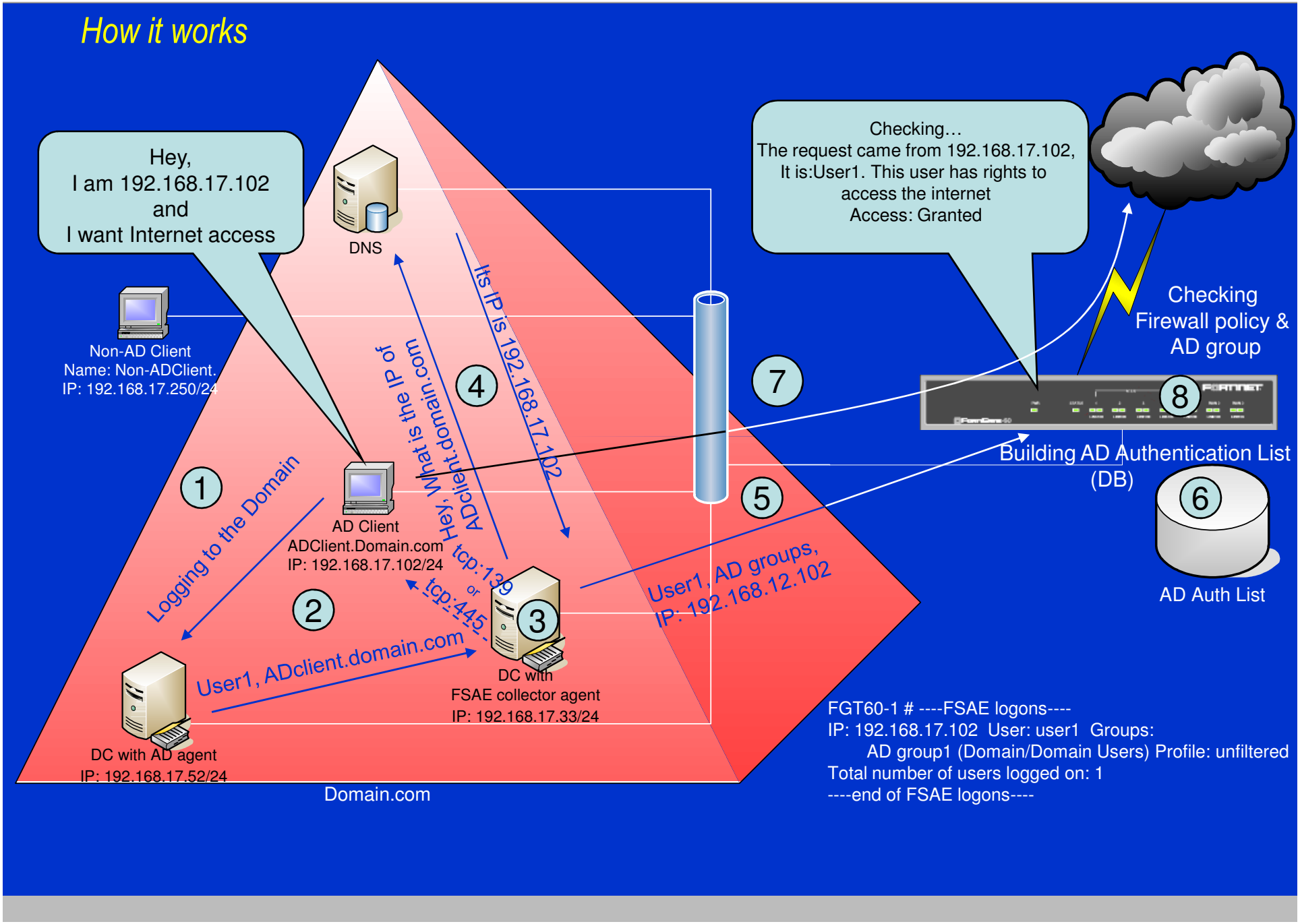
How it works



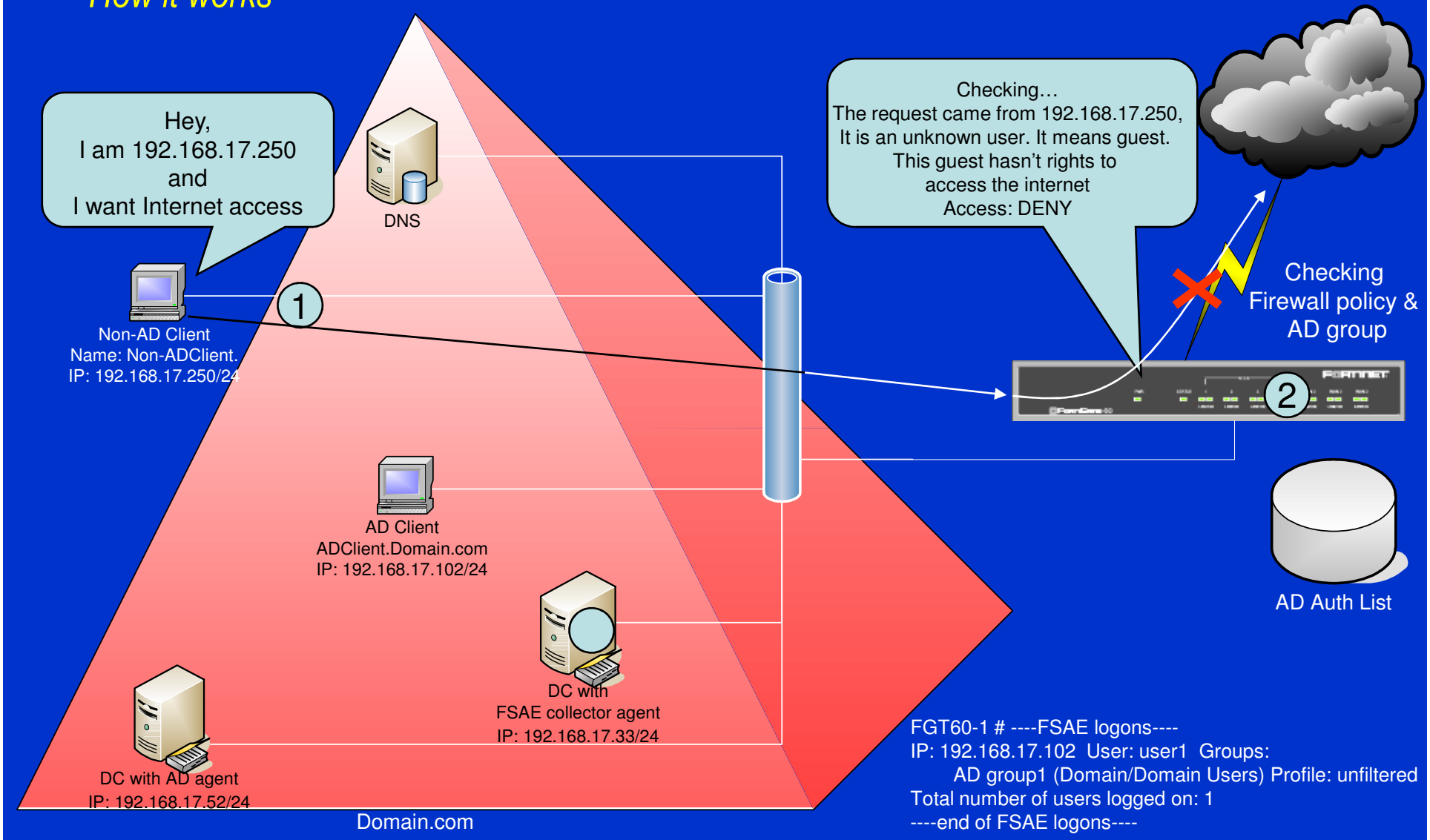

```
#diag debug authd fsae list
FGT60-1 # ----FSAE logons----
IP: 192.168.17.33  User: Administrator  Groups:
       AD group1 (Domain/Domain Users) Profile: unfiltered
IP: 192.168.17.102  User: user1  Groups:
       AD group1 (Domain/Domain Users) Profile: unfiltered
Total number of users logged on: 2
----end of FSAE logons----
```

*** The FGT will not build list for users do not belongs to AD groups configured in User->UserGroups->Active Directory**

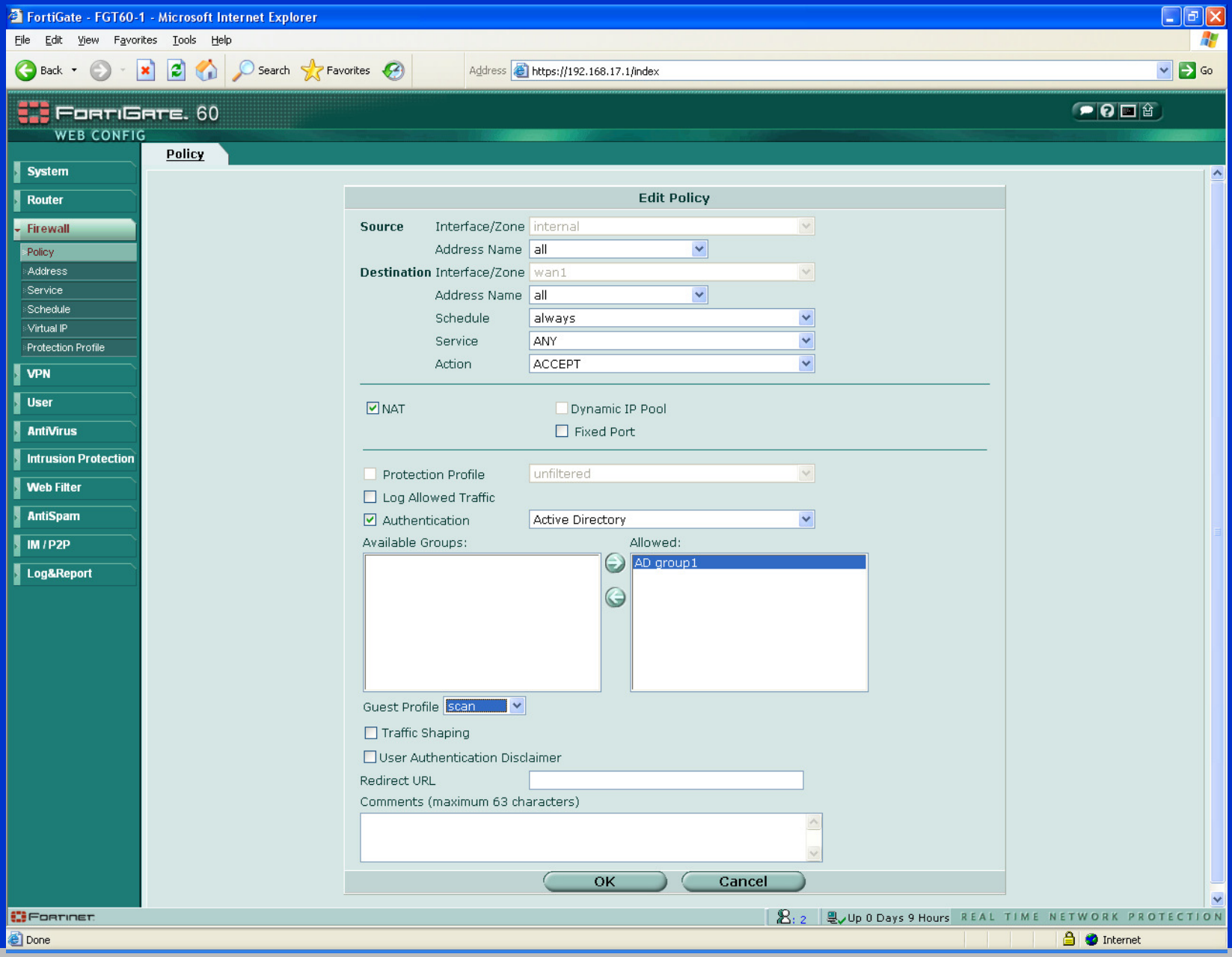
How it works


Hey,
I am 192.168.17.102
and
I want Internet access
Checking…
The request came from 192.168.17.102,
It is:User1. This user has rights to
access the internet
Access: Granted
DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
1
Logging to the Domain
2
User1, ADclient.domain.com
3
4
ADClient.domain.com, What is the IP of
tcp:139 or tcp:445, Hey,
Its IP is 192.168.17.102
5
User1, AD groups,
IP: 192.168.12.102
6
AD Auth List
7
8
Checking
Firewall policy &
AD group
Building AD Authentication List
(DB)
FGT60-1 # ----FSAE logons----
IP: 192.168.17.102 User: user1 Groups:
AD group1 (Domain/Domain Users) Profile: unfiltered
Total number of users logged on: 1
----end of FSAE logons----

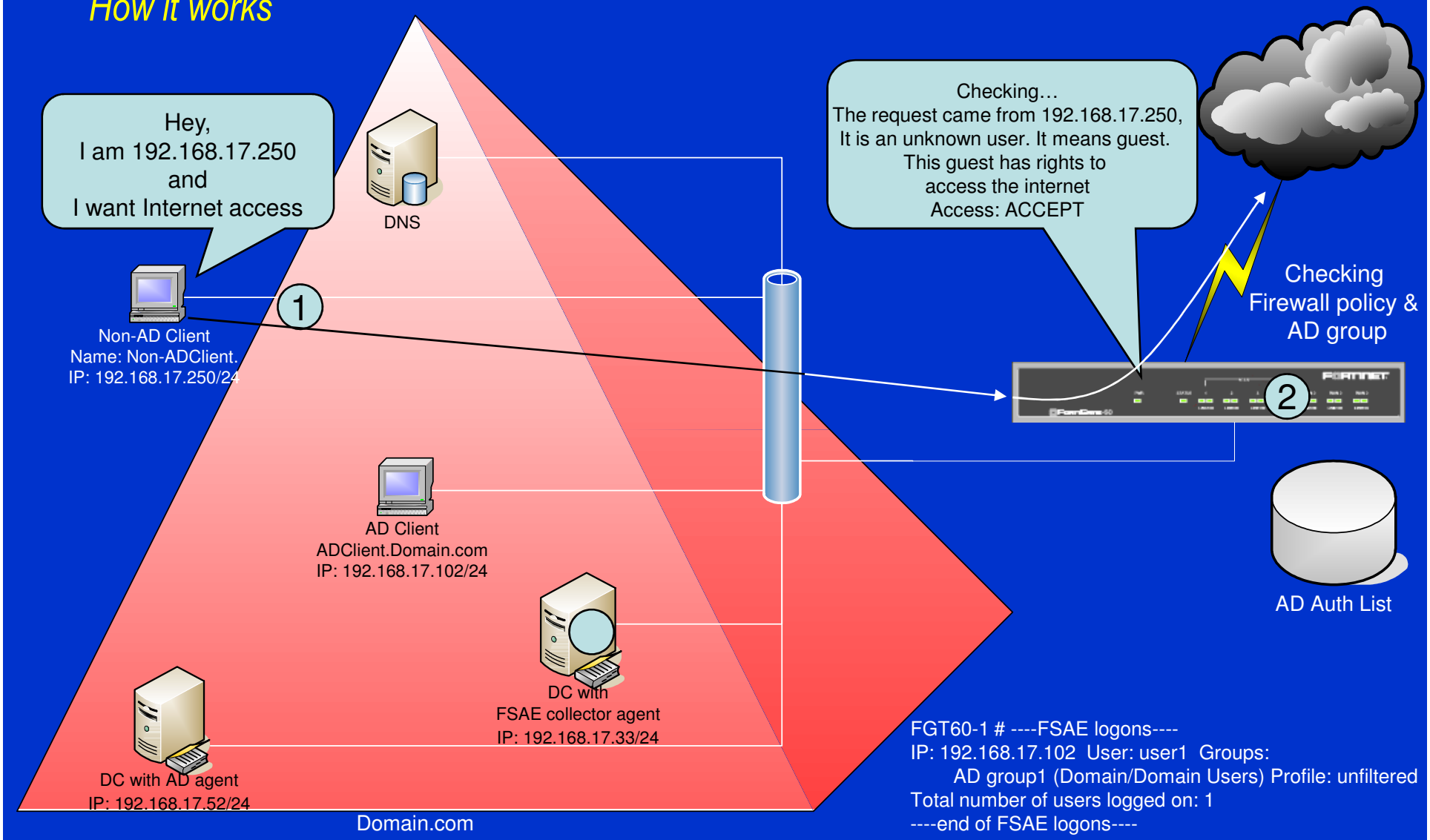
How it works


Hey,
I am 192.168.17.250
and
I want Internet access
DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
1
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
Checking…
The request came from 192.168.17.250,
It is an unknown user. It means guest.
This guest hasn't rights to
access the internet
Access: DENY
Checking
Firewall policy &
AD group
2
AD Auth List
FGT60-1 # ----FSAE logons----
IP: 192.168.17.102 User: user1 Groups:
AD group1 (Domain/Domain Users) Profile: unfiltered
Total number of users logged on: 1
----end of FSAE logons----

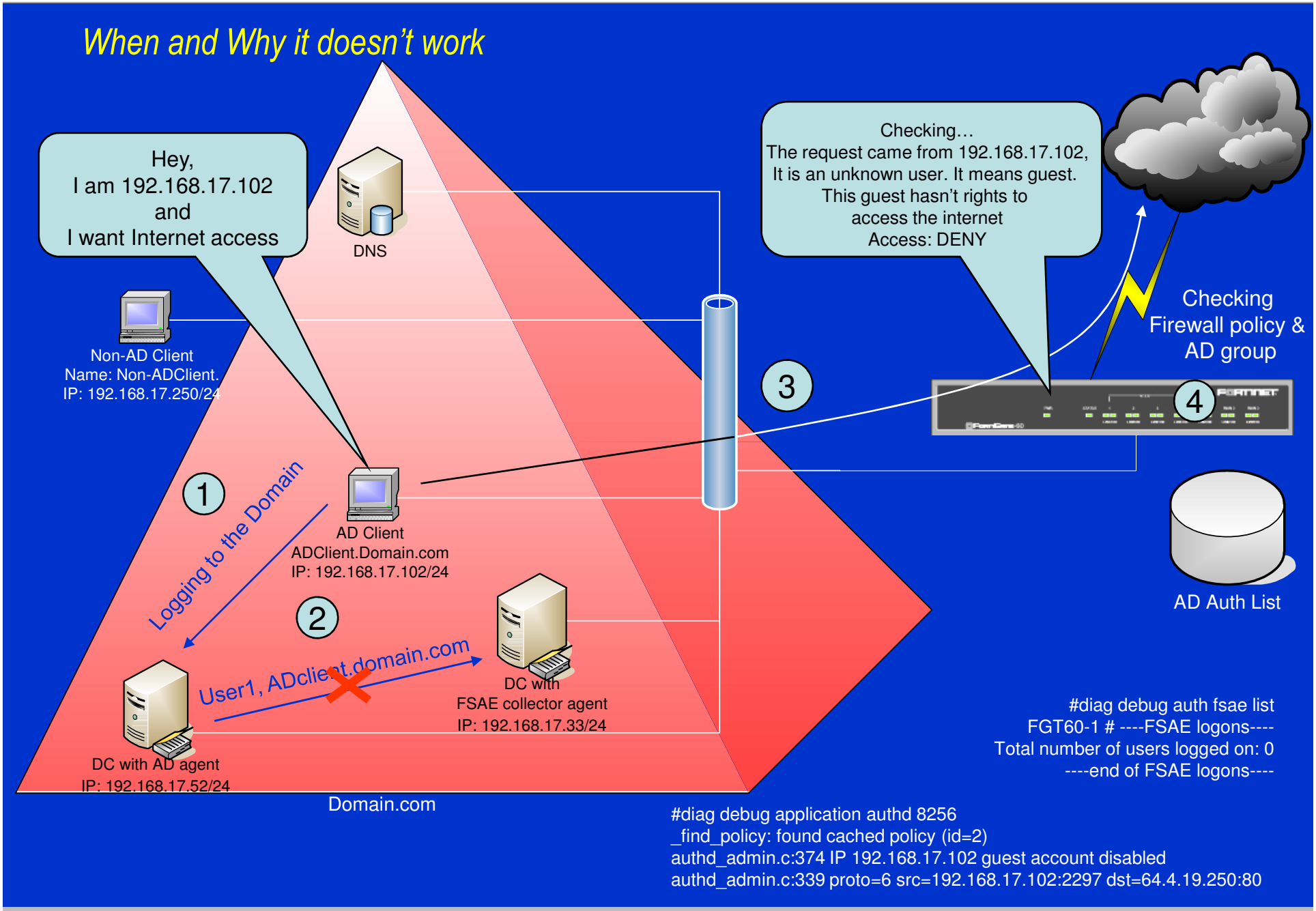
How it works


FortiGate - FGT60-1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.17.1/index
Go
FortiGate 60
WEB CONFIG
Policy
System
Router
Firewall
Policy
Address
Service
Schedule
Virtual IP
Protection Profile
VPN
User
AntiVirus
Intrusion Protection
Web Filter
AntiSpam
IM / P2P
Log&Report
Edit Policy
Source Interface/Zone internal
Address Name all
Destination Interface/Zone wan1
Address Name all
Schedule always
Service ANY
Action ACCEPT
NAT
Dynamic IP Pool
Fixed Port
Protection Profile unfiltered
Log Allowed Traffic
Authentication Active Directory
Available Groups:
Allowed:
AD group1
Guest Profile scan
Traffic Shaping
User Authentication Disclaimer
Redirect URL
Comments (maximum 63 characters)
OK
Cancel
Fortinet
Up 0 Days 9 Hours
REAL TIME NETWORK PROTECTION
Done
Internet

How it works


Hey,
I am 192.168.17.250
and
I want Internet access
DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
1
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
DC with
FSAE collector agent
IP: 192.168.17.33/24
DC with AD agent
IP: 192.168.17.52/24
Domain.com
Checking…
The request came from 192.168.17.250,
It is an unknown user. It means guest.
This guest has rights to
access the internet
Access: ACCEPT
Checking
Firewall policy &
AD group
2
AD Auth List
FGT60-1 # ----FSAE logons----
IP: 192.168.17.102 User: user1 Groups:
AD group1 (Domain/Domain Users) Profile: unfiltered
Total number of users logged on: 1
----end of FSAE logons----

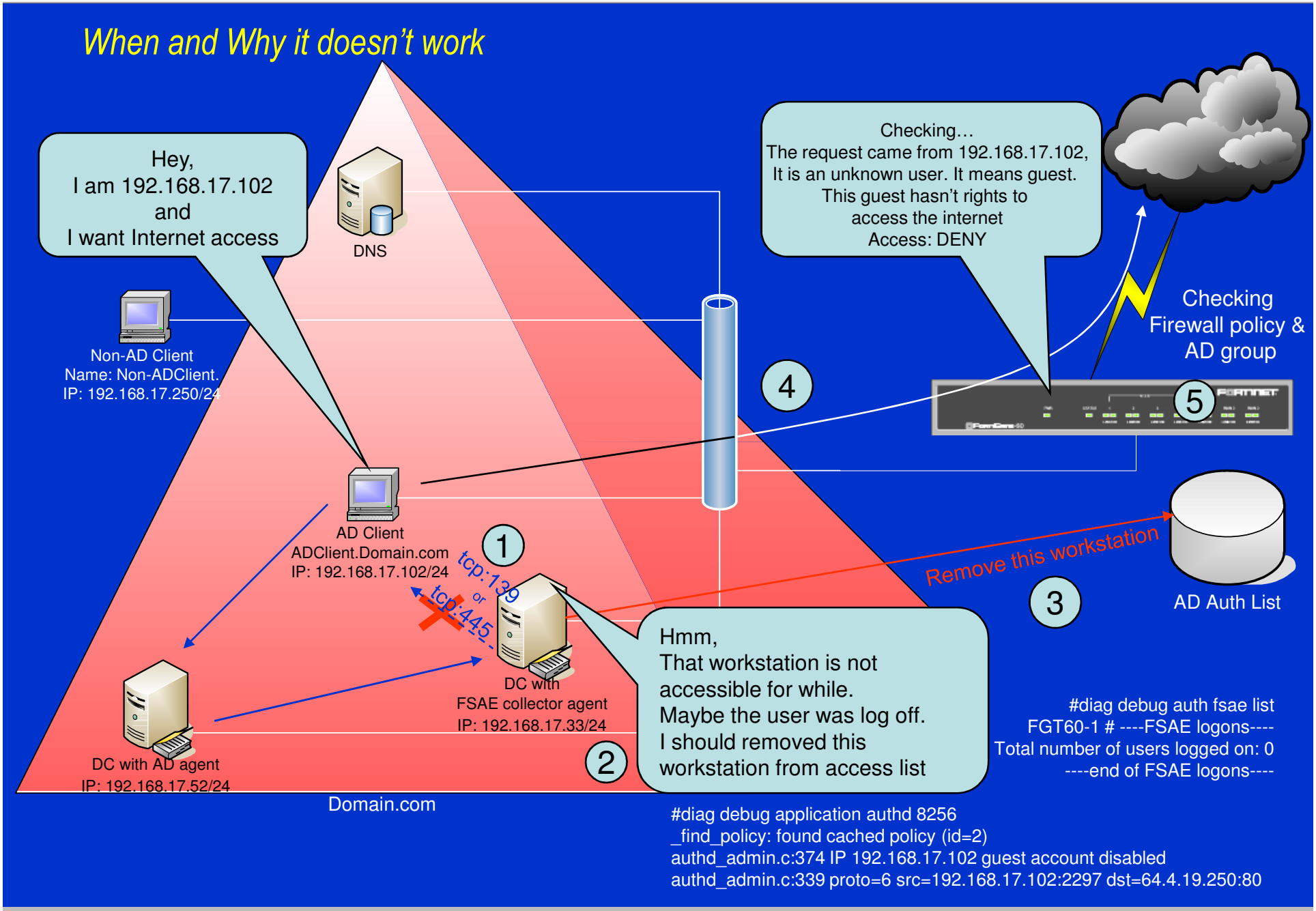
When and Why it doesn't work



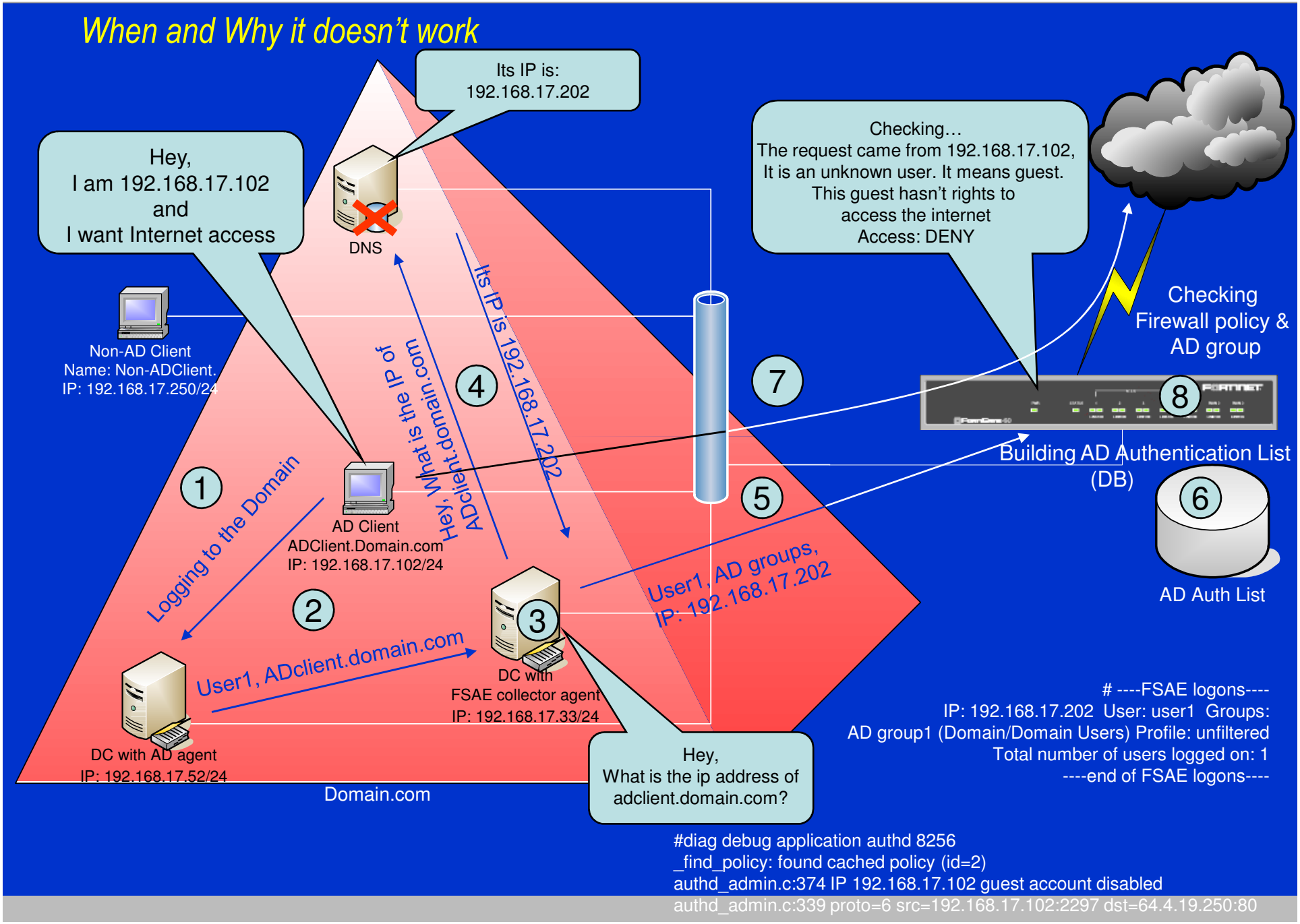
#diag debug auth fsae list
FGT60-1 # ----FSAE logons----
Total number of users logged on: 0
----end of FSAE logons----

#diag debug application authd 8256
_find_policy: found cached policy (id=2)
authd_admin.c:374 IP 192.168.17.102 guest account disabled
authd_admin.c:339 proto=6 src=192.168.17.102:2297 dst=64.4.19.250:80

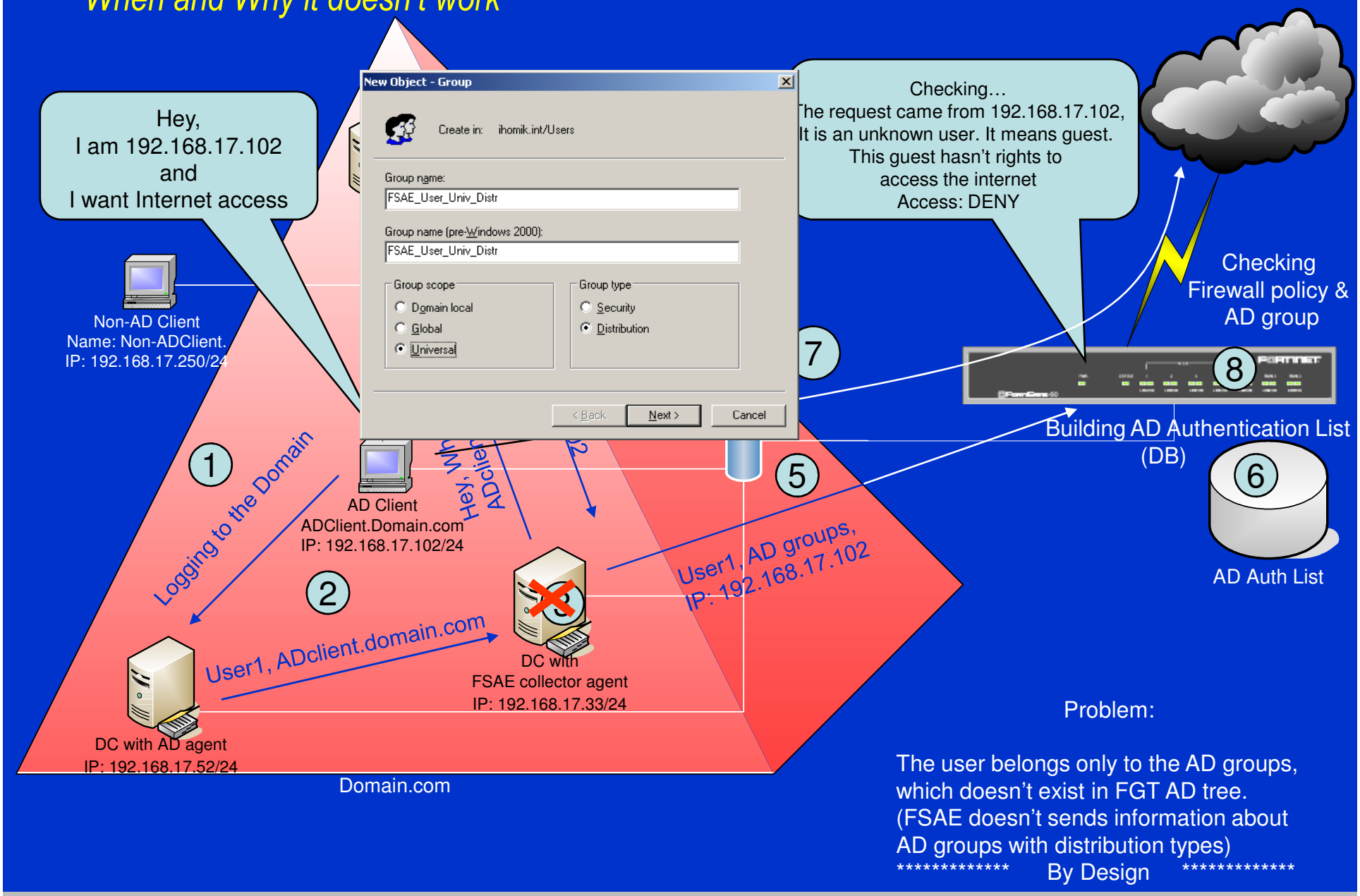
When and Why it doesn't work



When and Why it doesn't work



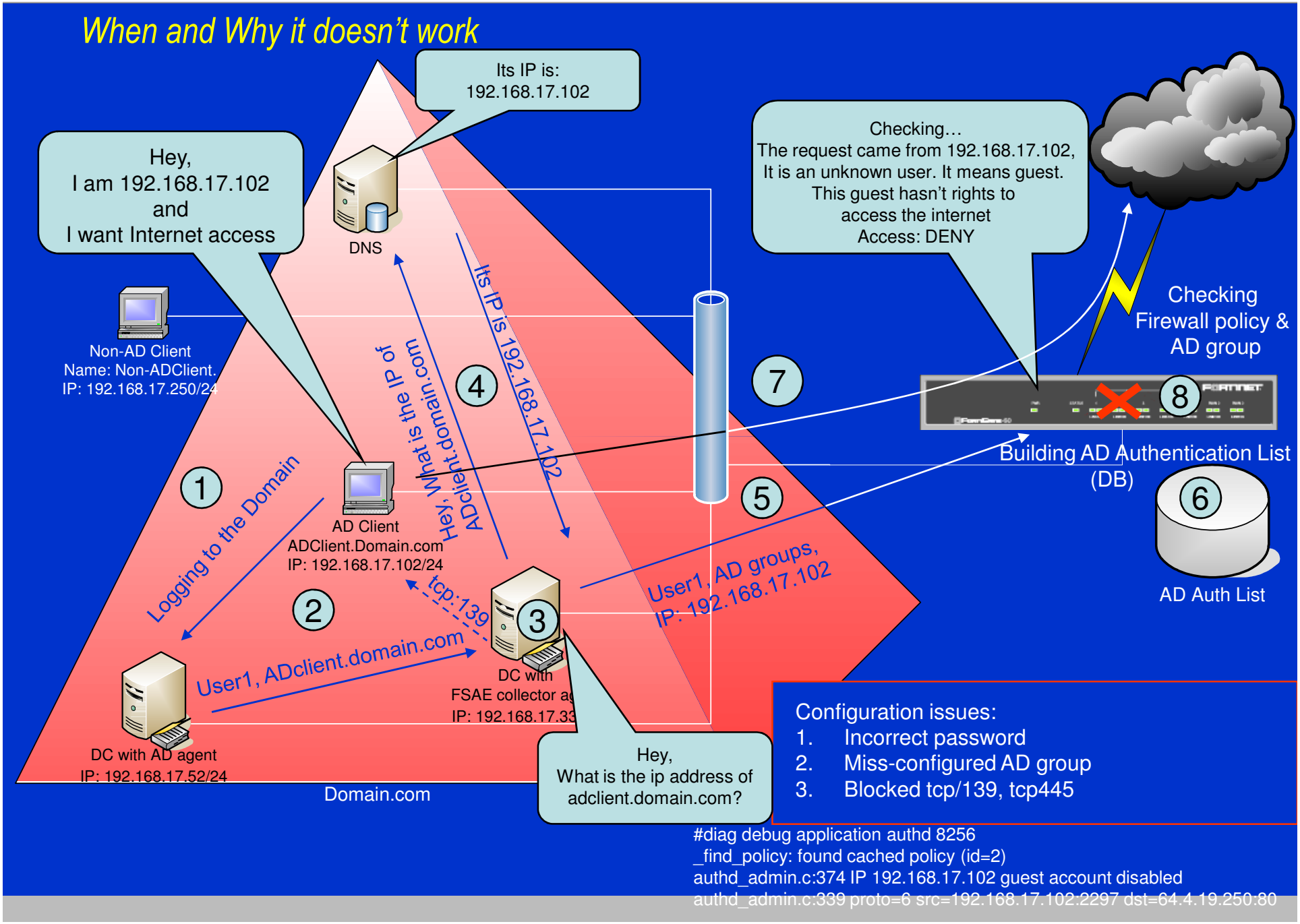
When and Why it doesn't work



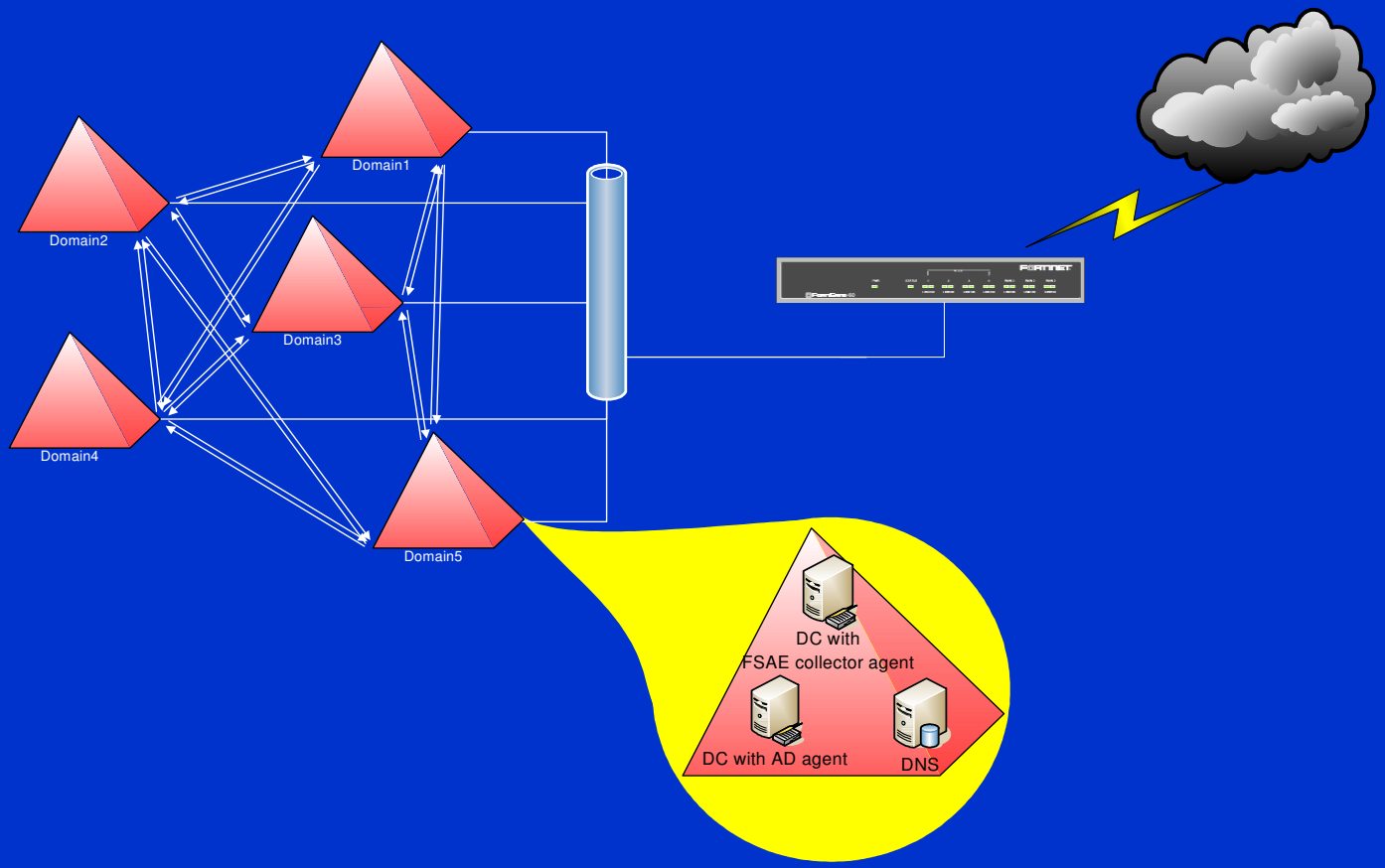
Problem:

The user belongs only to the AD groups, which doesn't exist in FGT AD tree. (FSAE doesn't sends information about AD groups with distribution types)

********** By Design **********


When and Why it doesn't work
Its IP is:
192.168.17.102
Hey,
I am 192.168.17.102
and
I want Internet access
DNS
Non-AD Client
Name: Non-ADClient.
IP: 192.168.17.250/24
Checking…
The request came from 192.168.17.102,
It is an unknown user. It means guest.
This guest hasn't rights to
access the internet
Access: DENY
Checking
Firewall policy &
AD group
Building AD Authentication List
(DB)
AD Auth List
1
Logging to the Domain
AD Client
ADClient.Domain.com
IP: 192.168.17.102/24
2
4
Hey, What is the IP of ADclient.domain.com
Its IP is 192.168.17.102
tcp:139
3
DC with
FSAE collector a
IP: 192.168.17.33
User1, ADclient.domain.com
DC with AD agent
IP: 192.168.17.52/24
Domain.com
5
User1, AD groups,
IP: 192.168.17.102
6
7
8
Hey,
What is the ip address of
adclient.domain.com?
Configuration issues:
1. Incorrect password
2. Miss-configured AD group
3. Blocked tcp/139, tcp445
#diag debug application authd 8256
_find_policy: found cached policy (id=2)
authd_admin.c:374 IP 192.168.17.102 guest account disabled
authd_admin.c:339 proto=6 src=192.168.17.102:2297 dst=64.4.19.250:80

Multi-domains environment



Troubleshooting commands

- #diag debug authd fsae list

  # ----FSAE logons----
  IP: 192.168.17.33 User: Administrator Groups: AD group1 (Domain/Domain Users) Profile: unfiltered
  IP: **192.168.17.102** User: **user1** Groups: **AD group1** (**Domain/Domain Users**) Profile: **unfiltered**
  Total number of users logged on: 2
  ----end of FSAE logons----

- #diag debug authd clear-logons

- #diag debug auth fsae refresh-logons

- #diag debug auth fsae refresh-groups

- #exec fsae refresh

- #diag debug application authd 8256

  # _process_logon[Win2003Srv]: user1 logged on_process_logoff[Win2003Srv]: **user1 logged** offreset_policy_timeout: clearing policy for **192.168.17.102** vfid=0_resolve_logon_profile[Win2003Srv]: **user1 (Domain/Domain Users**) --> unfilteredreset_policy_timeout: clearing policy for 192.168.17.102 vfid=0Fortigate-60 # diag debug authd clearFortigate-60 # exec fsae refresh - force an Active Directory user group refresh to the Fortigate

Troubleshooting commands

- #diag sniffer packet internal 'port 8000 and host <collector agent ip>' 3
- #diag sniffer packet internal 'port 8000 and host <collector agent ip>'

```
10.240308 192.168.17.1.1314 -> 192.168.17.33.8000: psh 3244212321 ack 2275748053
10.528406 192.168.17.33.8000 -> 192.168.17.1.1314: ack 3244212337
```

- #diag debug authd fsae server

```
# Server Name          Connection Status
-----------            -----------------
Win2003Srv             connected
```

- C:\echo %logonserver%"

Troubleshooting Tips

1. A specific workstation(s) constantly can't go to internet regardless of users logged into:
1.1 FGT$ diag debug app auth 8256 or FGT$ diag debug app auth 64
shows guest profile for the IP of this workstation:
_find_policy: found cached policy (id=3)
authd_admin.c:379 IP 192.168.12.231 guest account disabled
authd_admin.c:347 proto=6 src=192.168.12.231:1351 dst=207.46.199.93:443

1.2 Collector agent logs shows:
07/12/2007 13:02:33 [2176] failed to resolve workstation name to ip: WORKSTATION01
or
07/18/2007 10:58:03 [26380] DnsQuery() failed for WORKSTATION01, error code:9003

This scenario could happen when the workstation doesn't have proper DNS registration and the collector agent can't resolve the workstation name. (ex. No DNS record or there is DNS record but with incorrect IP)

2. A specific workstation(s) has intermittent problem accessing internet regardless of users logged into:
2.1 FGT$ diag debug auth fsae list , shows wrong user user logged into the workstation's IP
2.2 Collector agent logs shows:
07/12/2007 13:02:33 [2176] failed to resolve workstation name to ip: WORKSTATION01
or
07/18/2007 10:58:03 [26380] DnsQuery() failed for WORKSTATION01, error code:9003
This scenario is caused by multiple incorrect DNS registrations. The problem workstation doesn't have DNS records, but also there is another workstation (with internet access issue) with DNS record with the same IP address.

2.3 If the correct DNS records are configured and the problem appears for any logged users in certain time after the login and collector agent shows following records for this workstation:
07/18/2007 10:58:02 [26424] failed to connect to workstation: WORKSTATION01 (192.168.12.231)
It could be caused by firewall on the way between collector agent and the workstation or workstation's firewall. It seems the firewall is blocking 'TCP port 139 or 445' and collector agent is flushing the infor from the FGT.

Solutions are to open TCP port 139 or 445 .

Troubleshooting Tips

3. A specific workstation(s) has intermittent problem accessing internet depending of users logged into:

3.1 FGT$ diag debug app auth 8256 or FGT$ diag debug app auth 64
shows guest profile for the IP of this workstation:
_find_policy: found cached policy (id=3)
authd_admin.c:379 IP 192.168.12.231 guest account disabled
authd_admin.c:347 proto=6 src=192.168.12.231:1351 dst=207.46.199.93:443
Often this problem appears when the user doesn't belongs to any of AD groups specified into collector agent fortigate group filter. In this scenario collector agent will not pass information to the FGT.

Solution: Add the user to a group included into the filter. Or add the group which users belongs to into the filter. Or removed the filter.

4. A specific workstation(s) has intermittent problem accessing internet depending of users logged into:
4.1 FGT$ diag debug app auth 8256 or FGT$ diag debug app auth 64
shows guest profile for the IP of this workstation:
_find_policy: found cached policy (id=355)
authd_admin_read:390: no profile found for user user01 IP 192.168.12.58 (policy id 355)
message_loop: checking timeouts

Troubleshooting Tips

4.2 FGT$ diag debug auth fsae list
FGT$ ----FSAE logons----
IP: 192.168.12.47 User: user02 Groups:
DOMAIN01/ALL+DOMAIN01/FormsUsers+DOMAIN01/Certify+DOMAIN01/SharePointDesigners+DOMAIN01/PRT-5-HP8000+DOMAIN01/TorUsers+DOMAIN01/WebProxyUsers+DOMAIN01/ActivityUsers+DOMAIN01/TWorkUsers+DOMAIN01/CIDUsers+DOMAIN01/RRUsers+DOMAIN01/PDDUsers+DOMAIN01/InstActv+DOMAIN01/Domain Users+DOMAIN01/NinjaUsers+DOMAIN01/TrainServSupport+DOMAIN01/PDO-Sup+DOMAIN01/TS-Dir-Sup+DOMAIN01/PPS uploaders+DOMAIN01/DeaseCert+DOMAIN01/Internet Updaters+DOMAIN01/ContractsUsers+DOMAIN01/CourseUsers+DOMAIN01/Users
IP:192.168.12.58 User: user01 Groups:
domain01/ALL+domain01/TrainServReps+domain01/TorUsers+domain01/WebProxyUsers+domain01/TWorkUsers+domain01/CIDUsers+domain01/Domain Users+domain01/NinjaUsers+domain01/CourseUsers+domain01/Users
IP: 192.168.12.1 User: user03 Groups: DOMAIN01/Materials+DOMAIN01/ALL+DOMAIN01/Certify+DOMAIN01/PRT-XeroxDocUsers+DOMAIN01/ITSupport+DOMAIN01/Shippers+DOMAIN01/TrainServReps+DOMAIN01/TorUsers+DOMAIN01/IntranetUpdaters+DOMAIN01/AdminSoftwareInstallers+DOMAIN01/ActivityUsers+DOMAIN01/TWorkUsers+DOMAIN01/CIDUsers+DOMAIN01/InternetUsers+DOMAIN01/Domain Users+DOMAIN01/NinjaUsers+DOMAIN01/WebProxyUsers-Directors+DOMAIN01/TrainServSupport+DOMAIN01/PRT-NetAgentUsers+DOMAIN01/Policy Managers+DOMAIN01/IT Administrators+DOMAIN01/DOMAIN01 Dynamics Users+DOMAIN01/LabelRightUsers+DOMAIN01/PRT-5-PH8550+DOMAIN01/PRT-8-PH8550+DOMAIN01/Internet Updaters+DOMAIN01/ProjectUsers+DOMAIN01/LibraryUsers+DOMAIN01/CourseUsers+DOMAIN01/Remote Desktop Users+DOMAIN01/Users
Total number of users logged on: 3
----end of FSAE logons----
In this scenario User01 has problem and the problem is caused by configuration of the workstation. In most of the cases it is “manage my network passwords” on the workstation. The domain name is send in lower case. (Microsoft is not case sensitive, but FGT it is.)
Solution: This scenario could appear when collector agent build is prior b021. The solution is upgrade the collector agent to build 021 and it will convert all info into upper case prior to be send to the FGT.

4.3 If domain name is in upper case and the collector agent build is b021 or up, check the user belongs to AD group linked to the FGT’s groups and that groups in into ‘allow’ statement under fsae firewall policy

Troubleshooting Tips

5. Collector agent doesn't send logging events to the FGT from all users and sniff for traffic on port 8000 shows the syn requests going out but the rst ack comes back from the server.

5.1 FGT# diag sniff pack internal 'port 8000 and host 192.168.12.111'
interfaces=[internal]
filters=[port 8000 and host 192.168.12.111]
1.000288 192.168.12.5.4068 -> 192.168.12.111.8000: syn 667418663
1.001293 192.168.12.111.8000 -> 192.168.12.5.4068: rst 0 ack 667418664
6.000503 192.168.12.5.4070 -> 192.168.12.111.8000: syn 3777345912
6.002193 192.168.12.111.8000 -> 192.168.12.5.4070: rst 0 ack 3777345913
11.000275 192.168.12.5.4072 -> 192.168.12.111.8000: syn 3090423947
11.001238 192.168.12.111.8000 -> 192.168.12.5.4072: rst 0 ack 3090423948
16.000388 192.168.12.5.4074 -> 192.168.12.111.8000: syn 2235026108
16.001347 192.168.12.111.8000 -> 192.168.12.5.4074: rst 0 ack 2235026109

5.2 netstat –a –o –n doesn't show open port 8000
The problem is caused by Fortinet FSAE service is not running. It may happened that this services is configured with proper domain admin account.

6. Workstations have intermittent problem accessing internet depending of which DC controller is used for authentication. In most scenarios this appears to be a problem when more than two DCs have installed collector agents. The fortigate will query the first (top) collector agent configured under FGT's configuration. If the problem workstations do auth not to the 'first' DC and DC agents are missing configured the secondary AD agents were not able to send login even to the first collector agent.
Check registry: Collector agent should shows own IP and dcagent should also shows other collector agents:
[HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent]
"host"="192.168.12.111"
[HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\dcagent\ca]
"192.168.12.111"=dword:00001f42
"192.168.12.112"=dword:00001f42
Solution: Reinstall dcagent, if the it is miss configured