1.2 You have been asked to configure a remote VPN solution in the Internet Edge 1 layer of the network to support traffic from the Sales and Finance organizations. The requirements are as follows:

Clients must be able to establish remote VPN sessions with an idle timeout of one day.
Internal Database/Users must be used for the session authentication.

Only traffic that is destined for the Sales server, Finance server and NTP server must be encrypted.
Traffic between Sales PC and Finance PC should be allowed.

For the Sales organization, the second (or the third) address must be assigned from the block of 172.16.1.1 - 172.16.1.10/24.
For the Finance organization, the second (or the third) address must be assigned from the block of 172.16.1.11 - 172.16.1.20/24.

DACL must permit traffic destined to Sales server, Finance server, NTP server and DNS server.
DACL must permit ICMP traffic between Sales PC and Finance PC.

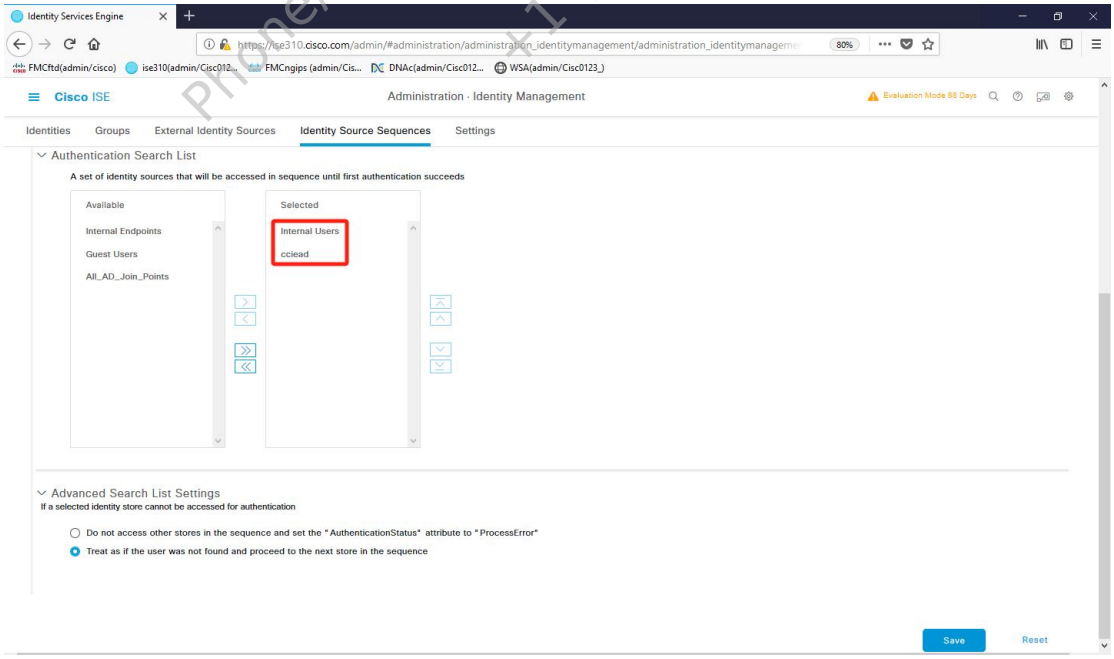
Updated Solution 1.2

ASA11v:

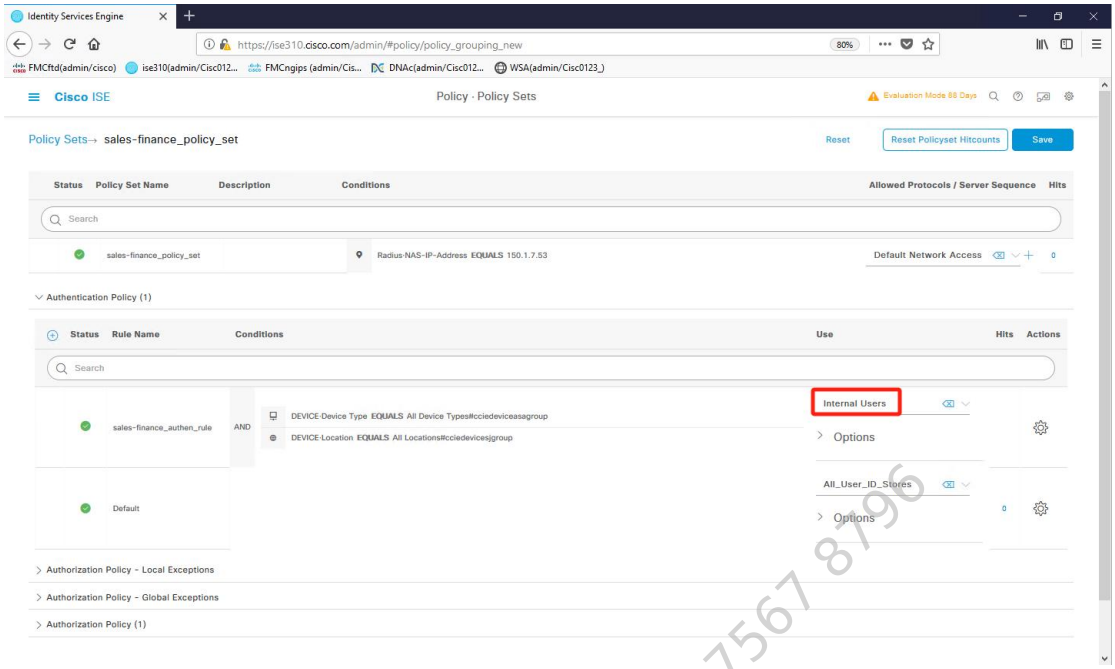
```
group-policy sales attributes
 vpn-idle-timeout 1440
group-policy finance attributes
 vpn-idle-timeout 1440
```

ISE (Login from Management PC):

Scenario 1: Still join AD, set Internal Users above cciead



Scenario 2: Use internal users only instead



For the specified IP address assignment (second or third), refer to the following settings accordingly:

...

...

1.3 You have been asked to deploy a remote VPN solution in the Internet Edge 2 layer of the network to support traffic that originates from a web browser. The requirements are as follows:

Clients must be able to establish remote VPN sessions using clientless SSL VPN tunnel with an idle timeout of one day.

Internal Database/Users must be used for the session authentication.

DNS domain lookup must use inside interface.

Only marketing and engineering clients can access their respective servers using their FQDN.

Updated Solution 1.3

ASA22v:

```
group-policy engineering attributes
 vpn-idle-timeout 1440
group-policy marketing attributes
 vpn-idle-timeout 1440
```

ISE (Login from Management PC):

Either Scenario 1 or Scenario 2: Refer to task 1.2

1.4 You have been asked to secure Richardson branch traffic for the Engineering server SSL access situated in HQ DC 2. The secure communication must use the site-to-site IPSec VPN model using Cisco Firepower Threat Defense. Your implementation must meet the following requirements:

Branch PCs need to access Engineering, NTP and DNS servers with pertaining ports.
IKEv2 tunnel keep-alive threshold must be 15 seconds with a retry interval of 3 seconds.
FTDs must have default network analysis policy of "Security Over Connectivity".
FTDs must be synchronized with the lab NTP server.
FTDs default rule must use block policy with logging disabled for FMC.

Updated Solution 1.4

. . .
. . .
. . .
. . .

4.5 You have been asked to deploy device administration function on R1 with using TACACS. The requirements are as follow:

ISE local users should be used as primary.
Username r1admin, password Cisc0123
Username r1operate, password Cisc0123

r1admin should be authorized with the following commands:
show running-config
show ntp status
configure terminal
inter G1
end
r1operate should be authorized with the following commands:
show running-config
show ntp status

Updated Solution 4.5

. . .
. . .