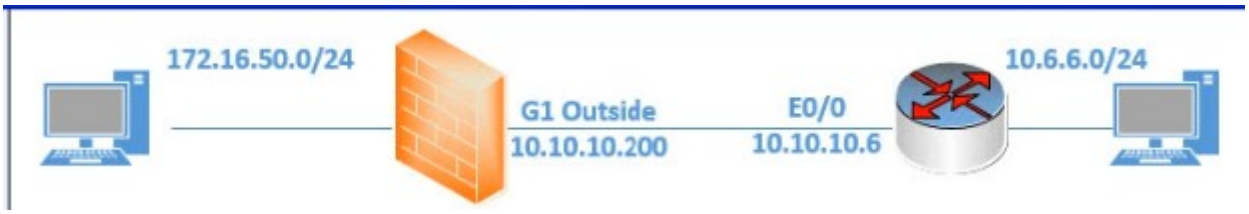
IKEv1 and IKEv2 VPNs between ASA and IOS:



! ASA1

enable

conf t

hostname ASA1
interface GigabitEthernet1
nameif inside
ip address 172.16.50.200 255.255.255.0
no shutdown
exit

ping 172.16.50.5

interface GigabitEthernet3
nameif outside
ip address 10.10.10.200 255.255.255.0
no shutdown
exit

ping 10.10.10.6

http server enable
http 0.0.0.0 0.0.0.0 outside

---

vpnsetup site-to-site steps

ping 10.10.10.6

object network INSIDE-NET
subnet 172.16.50.0 255.255.255.0
exit

object network R6-Network
subnet 10.6.6.0 255.255.255.0
exit

access-list CRY-ACL permit ip object INSIDE-NET object R6-Network

route outside 10.6.6.0 255.255.255.0 10.10.10.6 1

show route

crypto ikev1 policy 1
hash sha
authentication pre-share
group 5
lifetime 86400
encryption aes
exit

crypto ikev1 enable outside

crypto ikev2 policy 1
encryption aes-192 aes
integrity sha256 sha
prf sha256 sha
group 5 2
lifetime seconds 86400
exit

crypto ikev2 enable outside

crypto ipsec ikev1 transform-set Our-TSET esp-aes esp-sha-hmac

crypto ipsec ikev2 ipsec-proposal IPsecv2-AES
protocol esp encryption aes
protocol esp integrity sha-1 md5
exit

group-policy Group-A internal
group-policy Group-A attributes
vpn-tunnel-protocol ikev1 ikev2
exit

tunnel-group 10.10.10.6 type ipsec-l2l
tunnel-group 10.10.10.6 general-attributes
default-group-policy Group-A
exit

tunnel-group 10.10.10.6 ipsec-attributes

ikev1 pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
exit

```
crypto map Our-MAP 1 match address CRY-ACL
crypto map Our-MAP 1 set peer 10.10.10.6
crypto map Our-MAP 1 set ikev1 transform-set Our-TSET
crypto map Our-MAP 1 set ikev2 ipsec-proposal IPsecv2-AES
crypto map Our-MAP interface outside
```

! R6

```
enable
conf t
alias exec c config t
line con 0
no login
privi level 15
logging sync
no exec-timeout
no service time log
no service time debug
hostname R6
no service time log
no service time debug
ip route 0.0.0.0 0.0.0.0 10.10.10.200
int loop 0
ip add 6.6.6.6 255.255.255.255
int loop 1
ip add 10.6.6.6 255.255.255.0
ip ospf network point-to-point
ip ospf 1 area 0
int e0/0
ip address 10.10.10.6 255.255.255.0
no shut
exit
ip domain-name r6.cbtnuggets.com
ip http server
username admin privi 15 secret cisco
ip http authentication local
end
ping 10.10.10.200
```

! R6 IKEv1

```
conf t
crypto isakmp policy 1
```

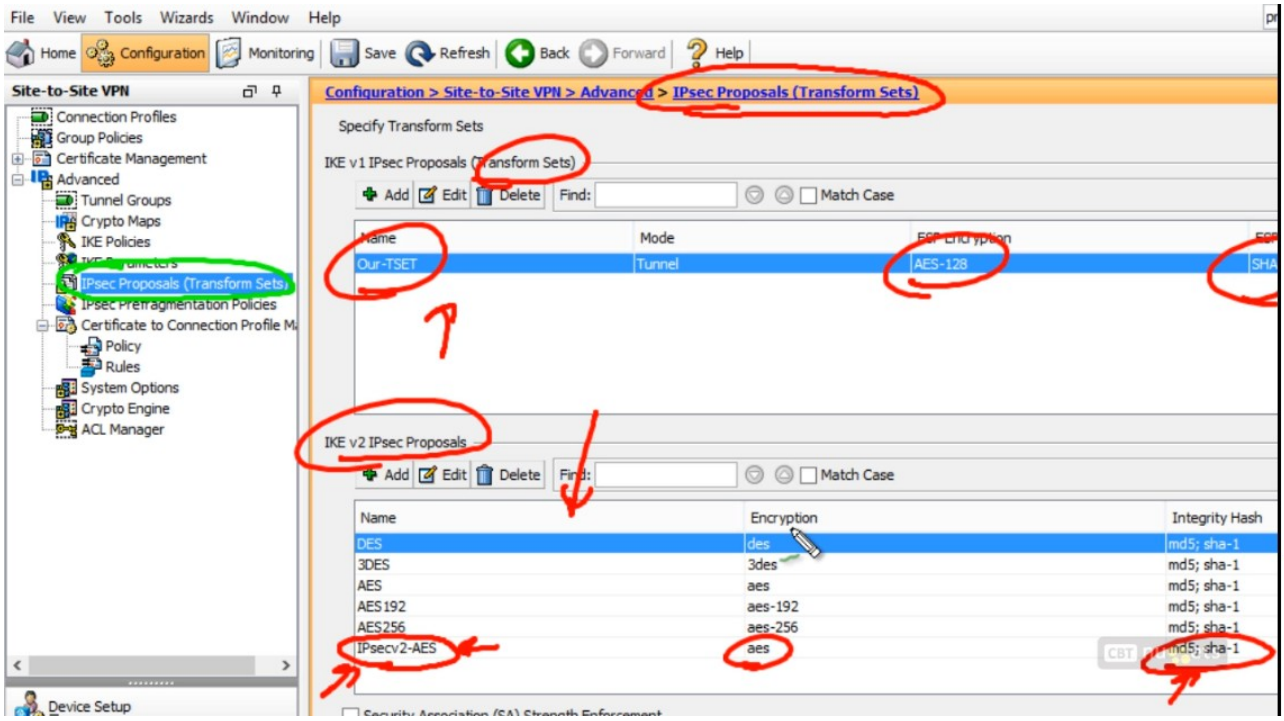
```
hash sha
authentication pre-share
group 5
lifetime 86400
encryption aes
exit

crypto isakmp key cisco123 address 10.10.10.200

crypto ipsec transform-set Our-TSET esp-aes esp-sha-hmac
exit

ip access-list extended CRY-ACL
permit ip 10.6.6.0 0.0.0.255 172.16.50.0 0.0.0.255
exit

crypto map Our-MAP 1 ipsec-isakmp
match address CRY-ACL
set peer 10.10.10.200
set transform-set Our-TSET
exit

int e 0/0
crypto map Our-MAP
end

show crypto isakmp sa

show crypto map

ping 172.16.50.5 source 10.6.6.6

show crypto isakmp sa

show crypto session

show crypto engine connections active
```

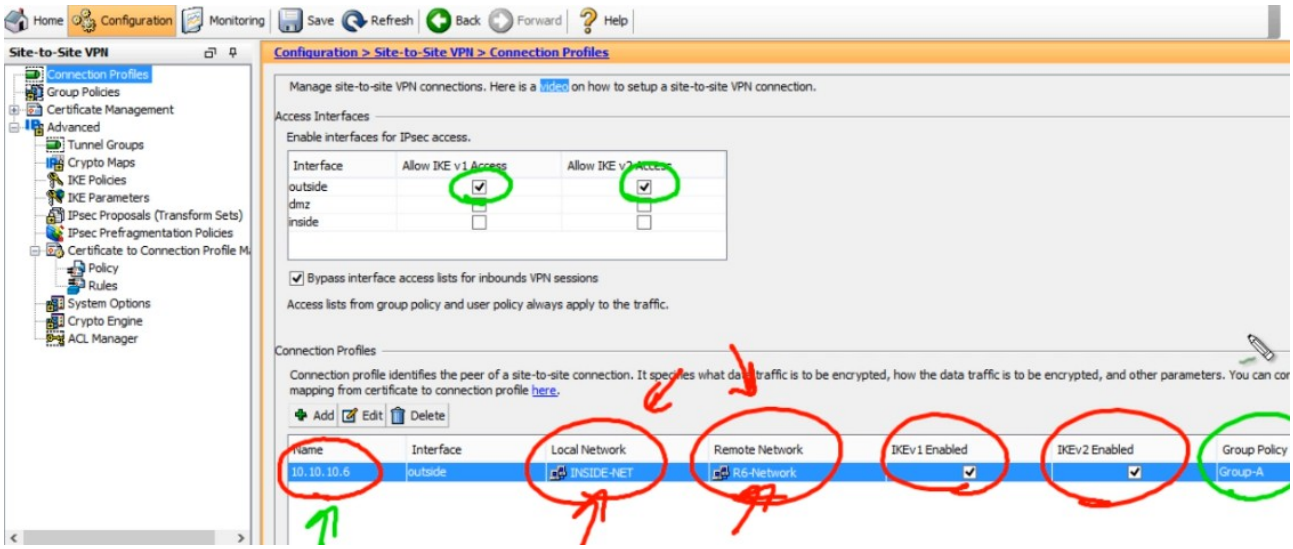
! R6 IKEv2

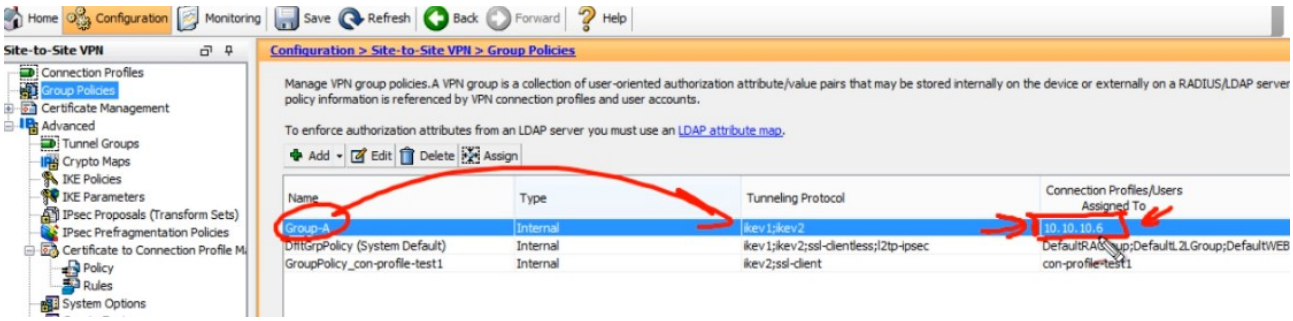
```
conf t

int e0/0
no crypto map
exit

crypto ikev2 proposal IKEv2-Proposal
encryption aes-cbc-128
integrity sha1
group 5 2
exit
```

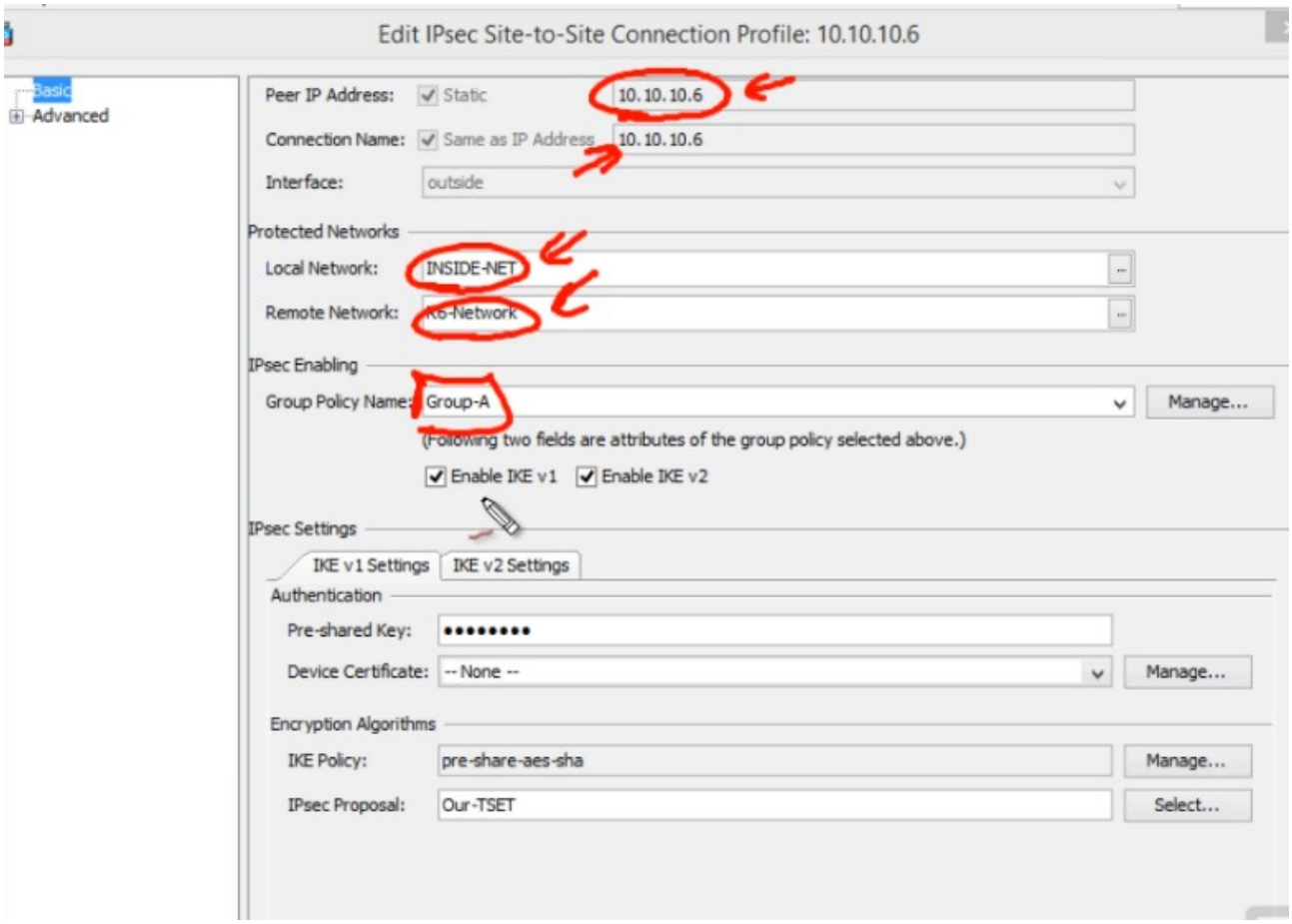
```
crypto ikev2 policy default
proposal IKEv2-Proposal
exit

crypto ikev2 keyring KEYRING1
peer ASA1
address 10.10.10.200
identity address 10.10.10.200
pre-shared-key local cisco123
pre-shared-key remote cisco123
exit
exit

crypto ikev2 profile IKEv2-Profile
match address local 10.10.10.6
match identity remote address 10.10.10.200
authentication remote pre-share
authentication local pre-share
keyring local KEYRING1
exit


crypto ipsec transform-set Our-v2TSET esp-aes esp-sha-hmac
exit

ip access-list extended 102
permit ip 10.6.6.0 0.0.0.255 172.16.50.0 0.0.0.255
exit

crypto map Our-v2Map 1 ipsec-isakmp
match address 102
set peer 10.10.10.200
set transform-set Our-v2TSET
set ikev2-profile IKEv2-Profile
exit

int e 0/0
crypto map Our-v2Map
end

show crypto session

ping 172.16.50.5 source 10.6.6.6

show crypto session

show crypto ikev2 sa

show crypto ikev2 sa detail

show crypto engine connections active
```

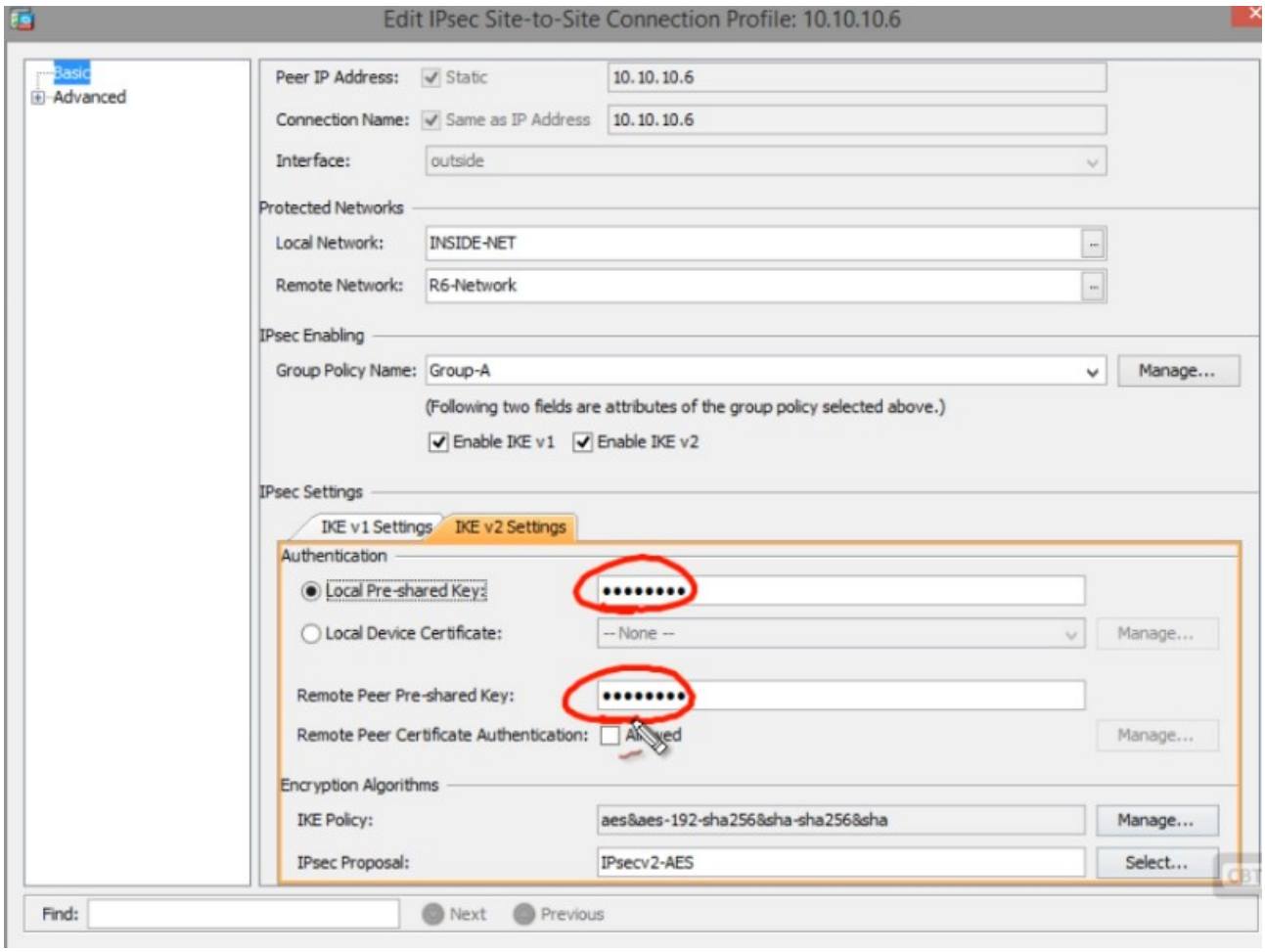
ASDM verification:

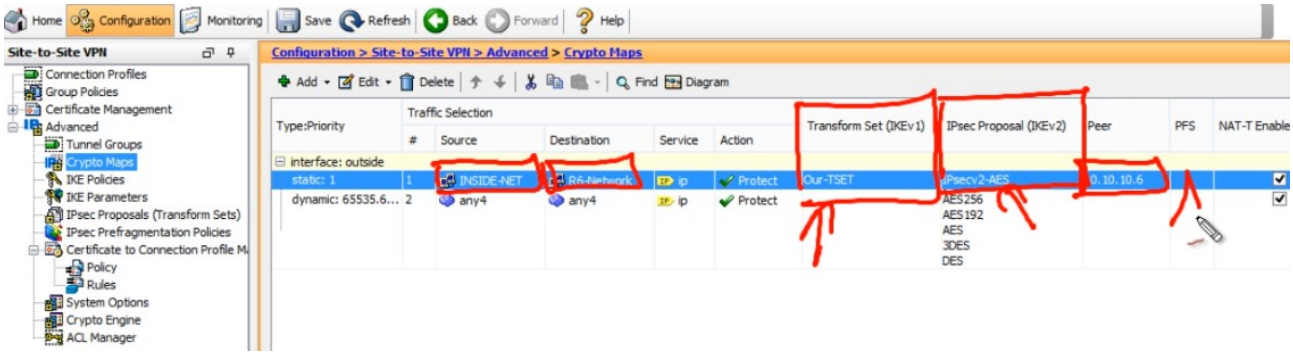







Edit IPsec Site-to-Site Connection Profile: 10.10.10.6
Basic
Advanced
Peer IP Address:
Static
10.10.10.6
Connection Name:
Same as IP Address
10.10.10.6
Interface:
outside
Protected Networks
Local Network:
INSIDE-NET
Remote Network:
R6-Network
IPsec Enabling
Group Policy Name:
Group-A
Manage...
(Following two fields are attributes of the group policy selected above.)
Enable IKE v1
Enable IKE v2
IPsec Settings
IKE v1 Settings
IKE v2 Settings
Authentication
Pre-shared Key:
Device Certificate:
-- None --
Manage...
Encryption Algorithms
IKE Policy:
pre-share-aes-sha
Manage...
IPsec Proposal:
Our-TSET
Select...


Edit IPsec Site-to-Site Connection Profile: 10.10.10.6
Basic
Advanced
Peer IP Address:
Static
10.10.10.6
Connection Name:
Same as IP Address
10.10.10.6
Interface:
outside
Protected Networks
Local Network:
INSIDE-NET
Remote Network:
R6-Network
IPsec Enabling
Group Policy Name:
Group-A
Manage...
(Following two fields are attributes of the group policy selected above.)
Enable IKE v1
Enable IKE v2
IPsec Settings
IKE v1 Settings
IKE v2 Settings
Authentication
Local Pre-shared Key:
Local Device Certificate:
-- None --
Manage...
Remote Peer Pre-shared Key:
Remote Peer Certificate Authentication:
Manage...
Encryption Algorithms
IKE Policy:
aes&aes-192-sha256&sha-sha256&sha
Manage...
IPsec Proposal:
IPsecv2-AES
Select...
Find:
Next
Previous


Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile M
Policy
Rules
System Options
Crypto Engine
ACL Manager
Configuration > Site-to-Site VPN > Advanced > Crypto Maps
Add
Edit
Delete
Find
Diagram
Type:Priority
Traffic Selection
#
Source
Destination
Service
Action
Transform Set (IKEv1)
IPsec Proposal (IKEv2)
Peer
PFS
NAT-T Enable
interface: outside
static: 1
1
INSIDE-NET
R4-Network
ip
Protect
Our-TSET
IPsecv2-AES
0.10.10.6
dynamic: 65535.6...
2
any4
any4
ip
Protect
AES256
AES192
AES
3DES
DES