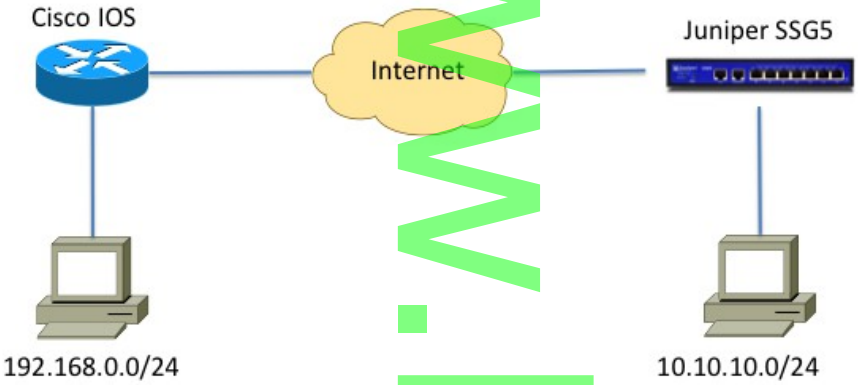
IPSec VPN Site-to-Site Juniper SSG5 to Cisco IOS



Phase 1

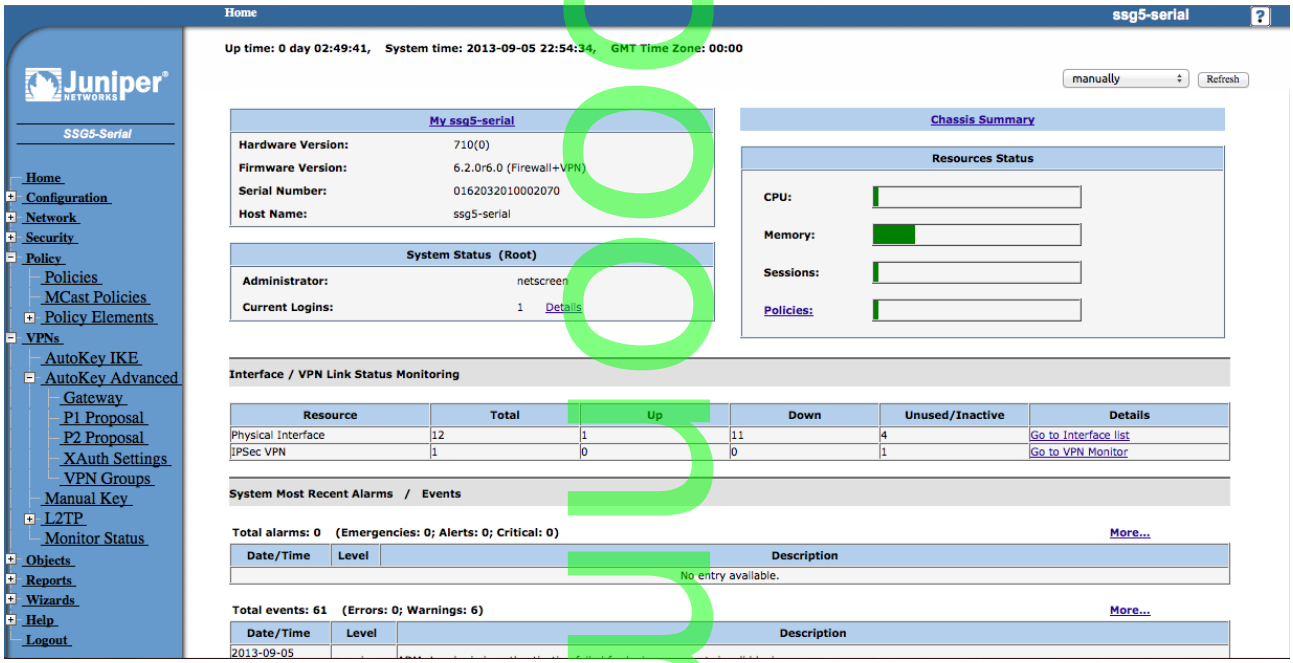
- pre-shared key 112233
- DH Group2
- Encryption 3DES
- Hash MD5
- Lifetime 28800
- Main mode
- Enable NAT-T

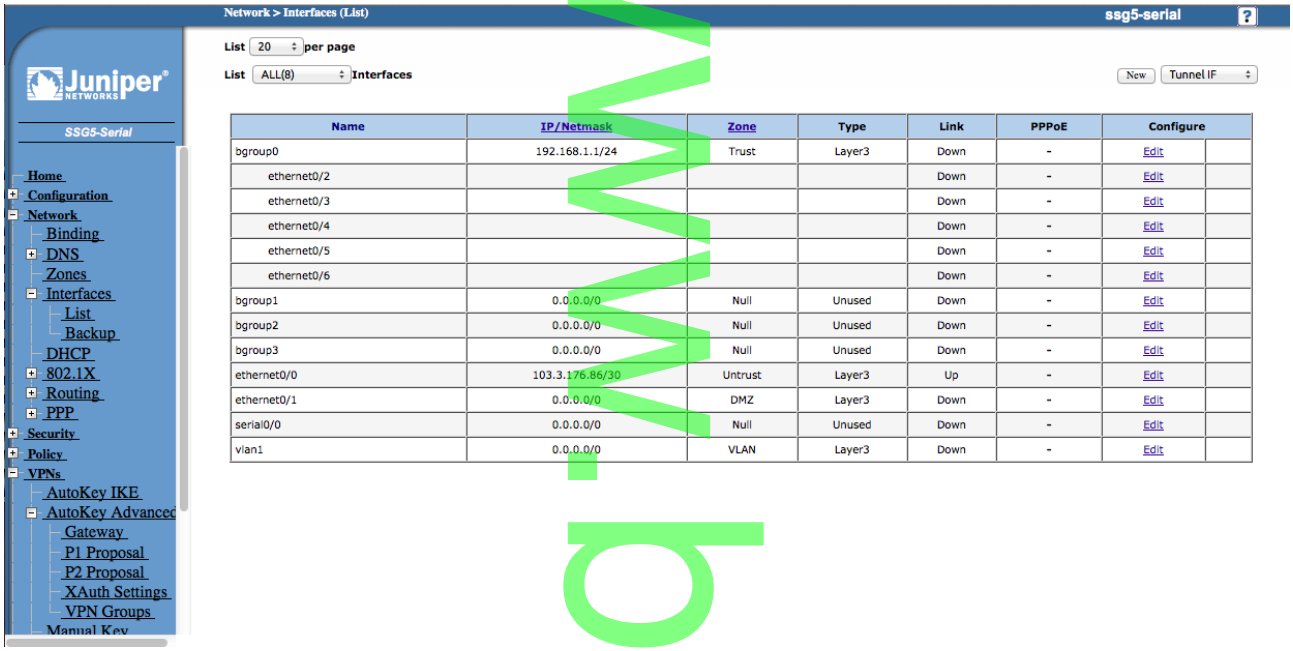
Phase 2

- No PFS
- ESP 3DES MD5
- Lifetime 3600

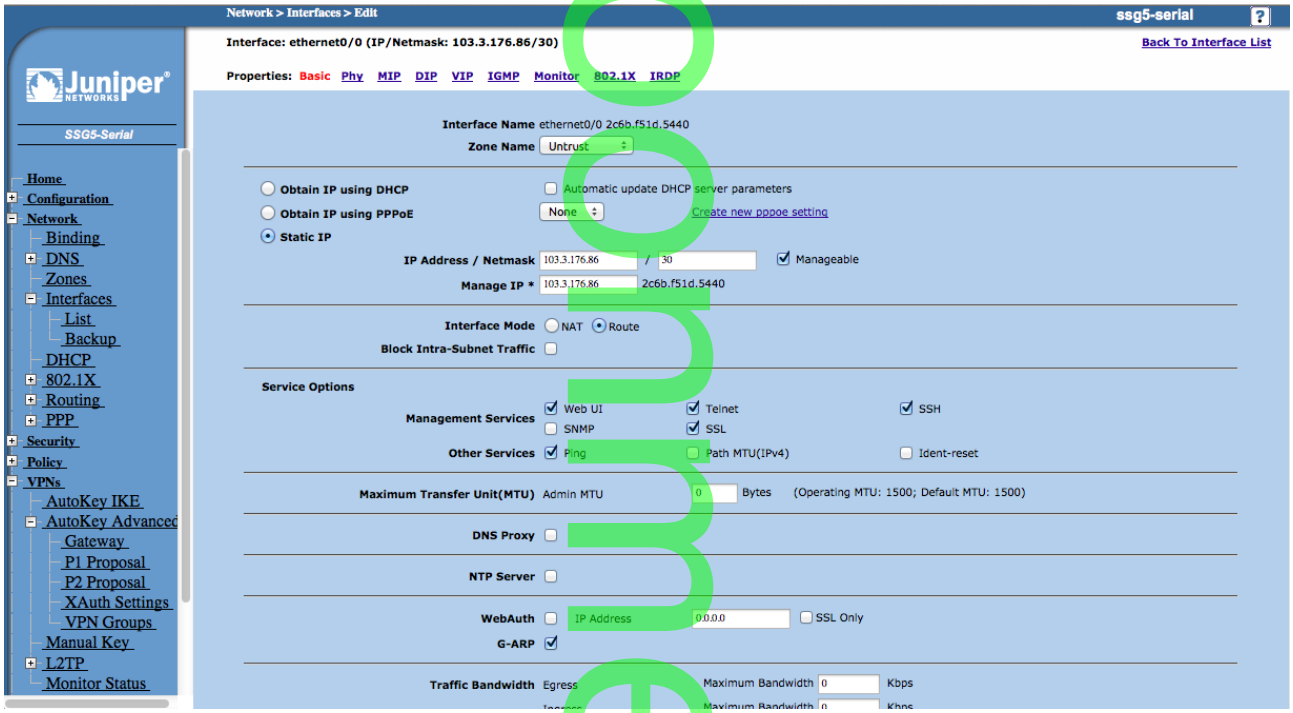
[Juniper SSG5]

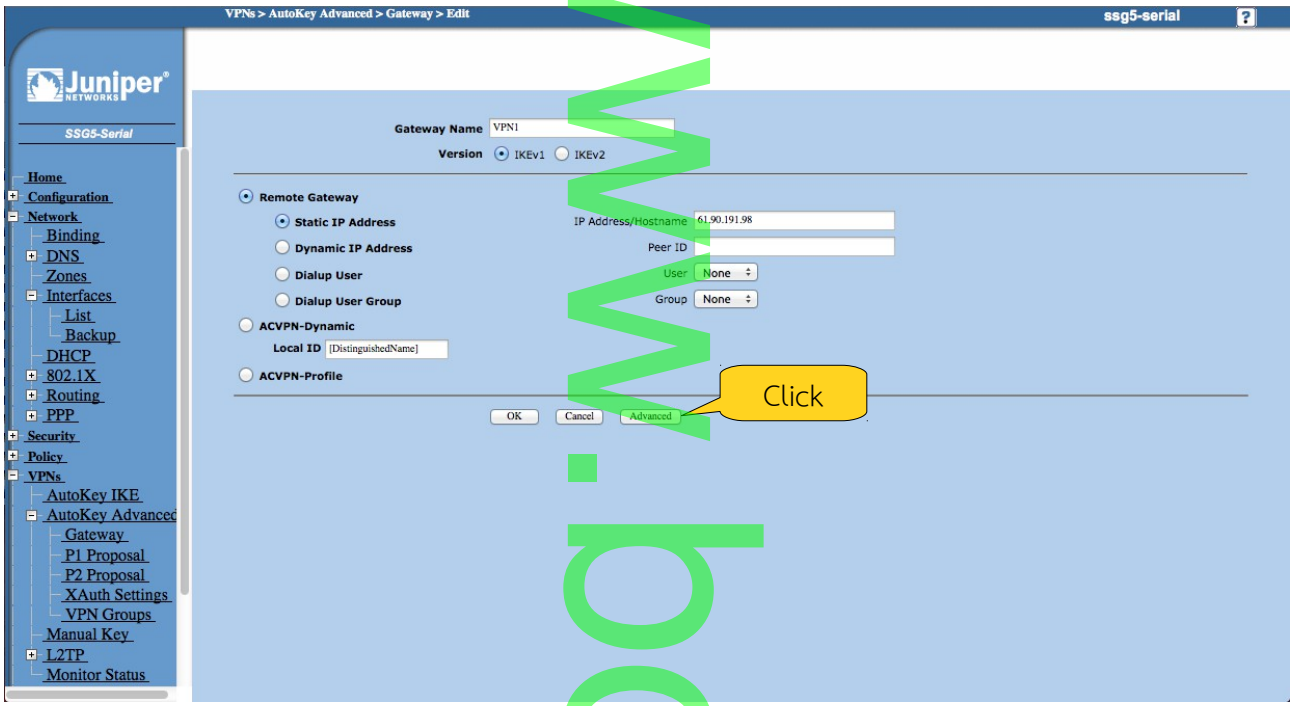
set admin password <PASSWORD>
set interface ethernet0/0 ip 103.3.176.86/30
set interface ethernet0/0 ip manageable
set interface ethernet0/0 manage ping
set interface ethernet0/0 manage ssh
set interface ethernet0/0 manage telnet
set interface ethernet0/0 manage web
set route 0.0.0.0/0 gateway 103.3.176.85

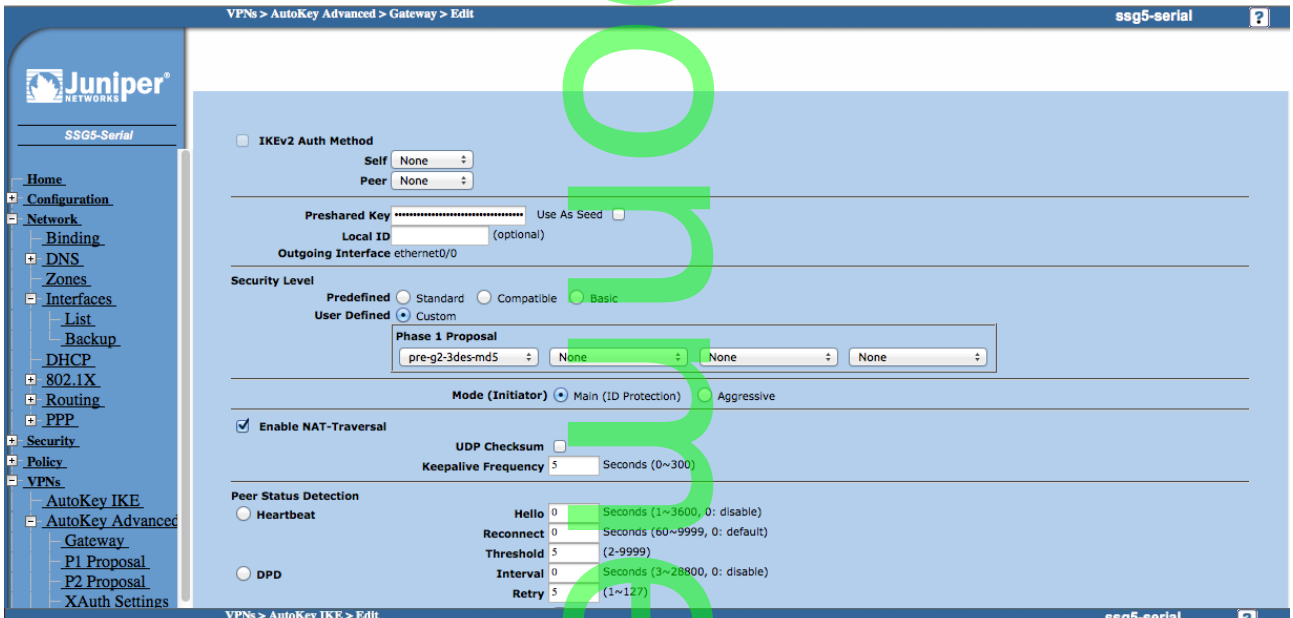


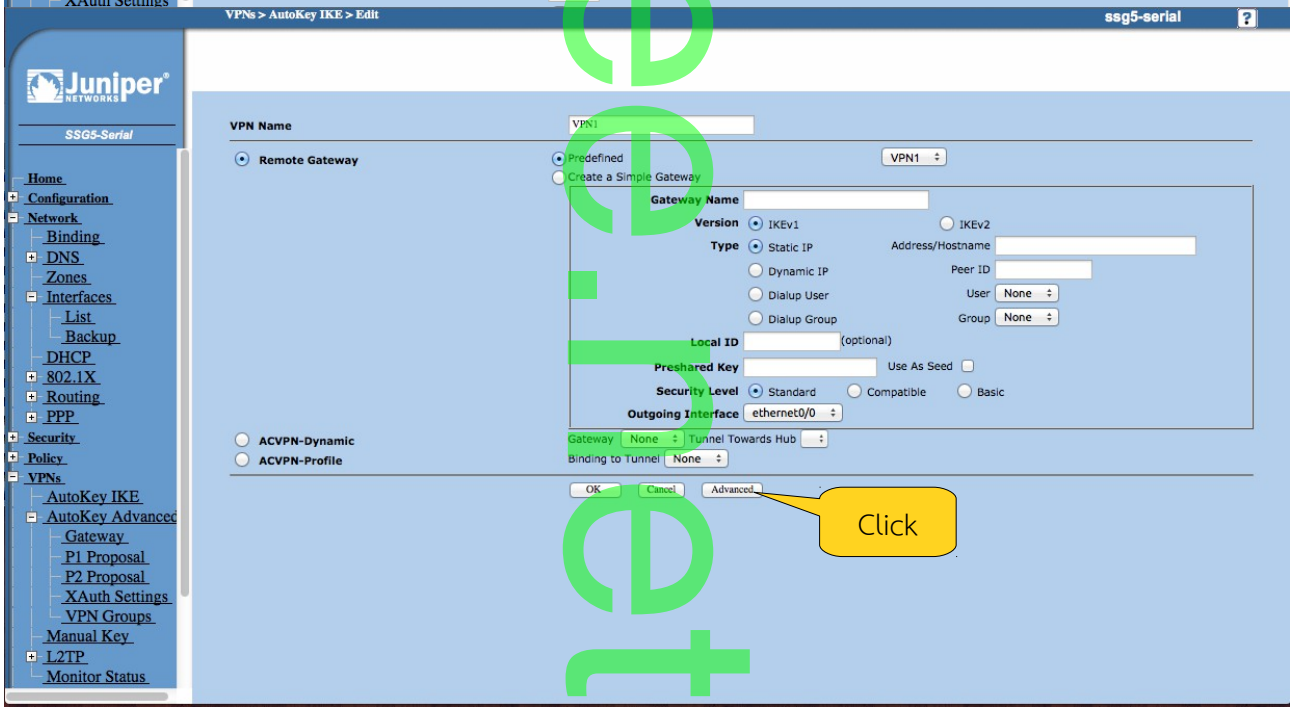


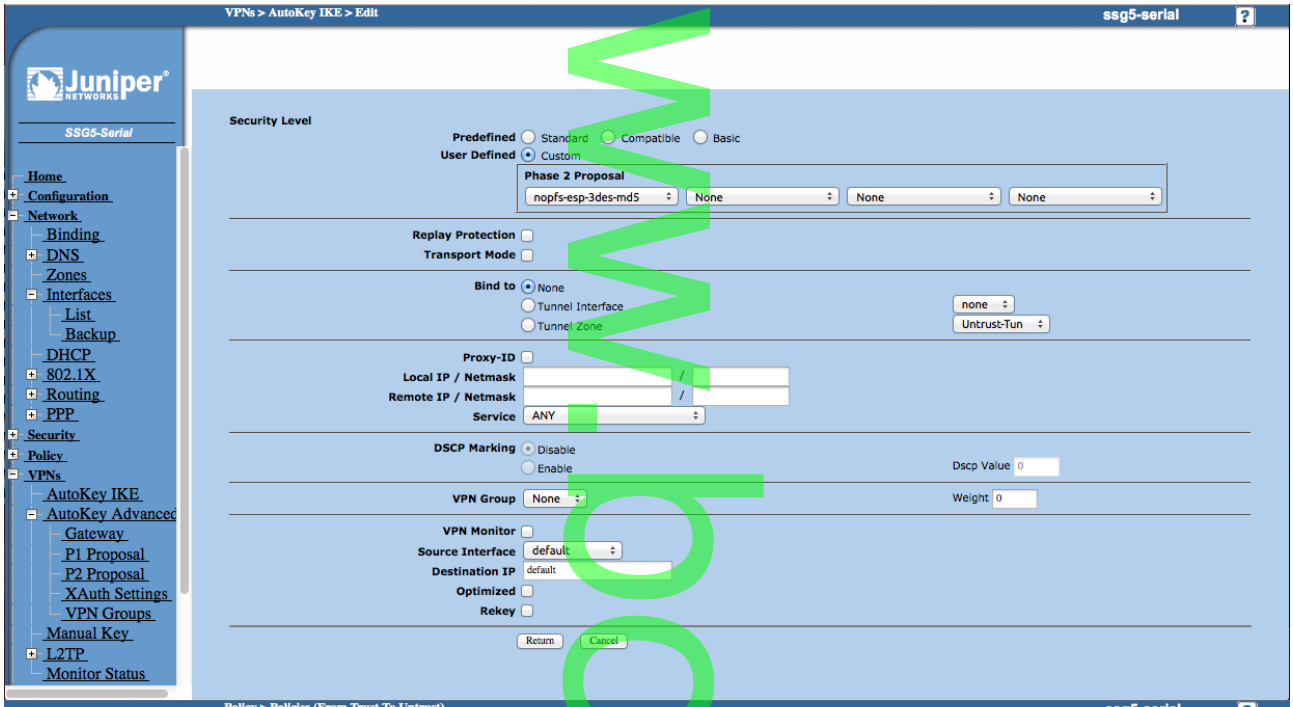
Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Down	-	Edit
ethernet0/2				Down	-	Edit
ethernet0/3				Down	-	Edit
ethernet0/4				Down	-	Edit
ethernet0/5				Down	-	Edit
ethernet0/6				Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	103.3.176.86/30	Untrust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

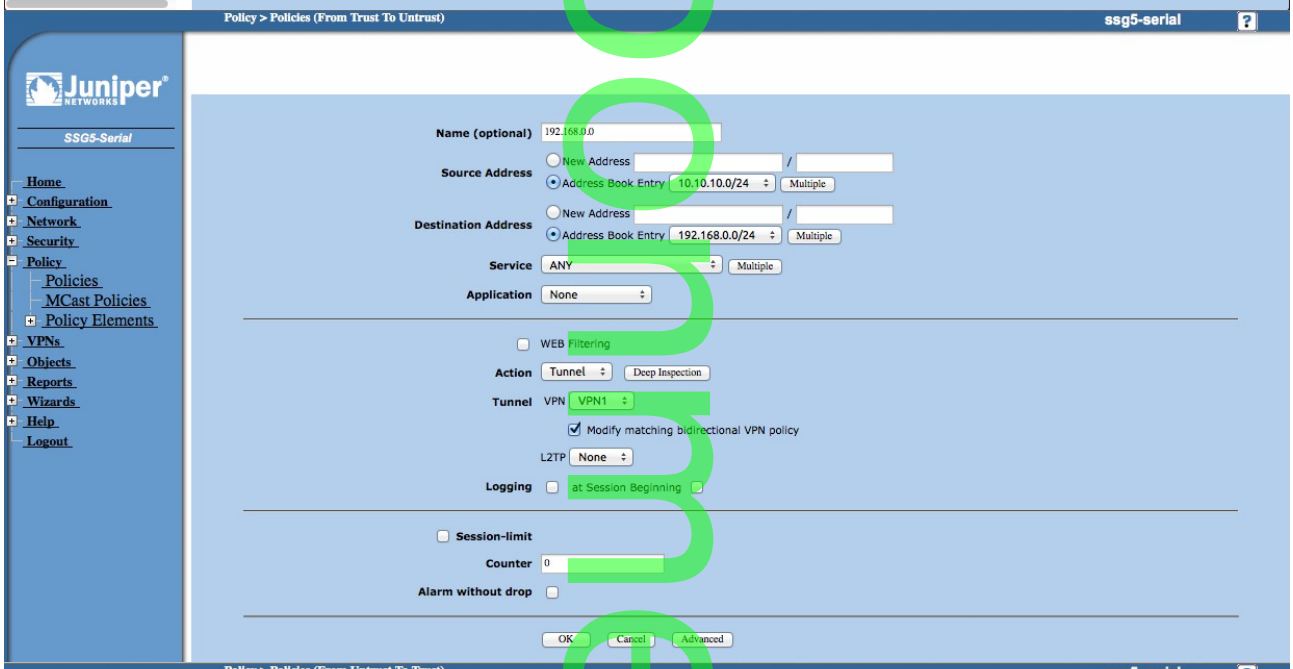


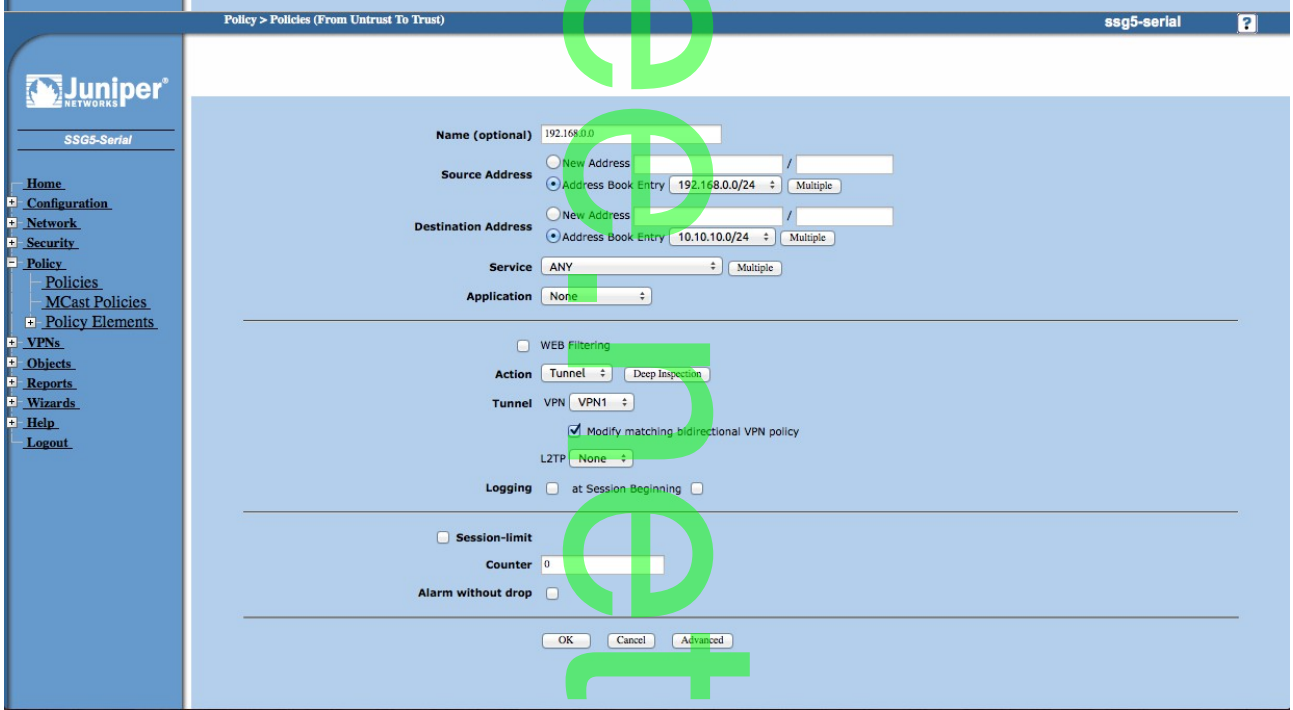


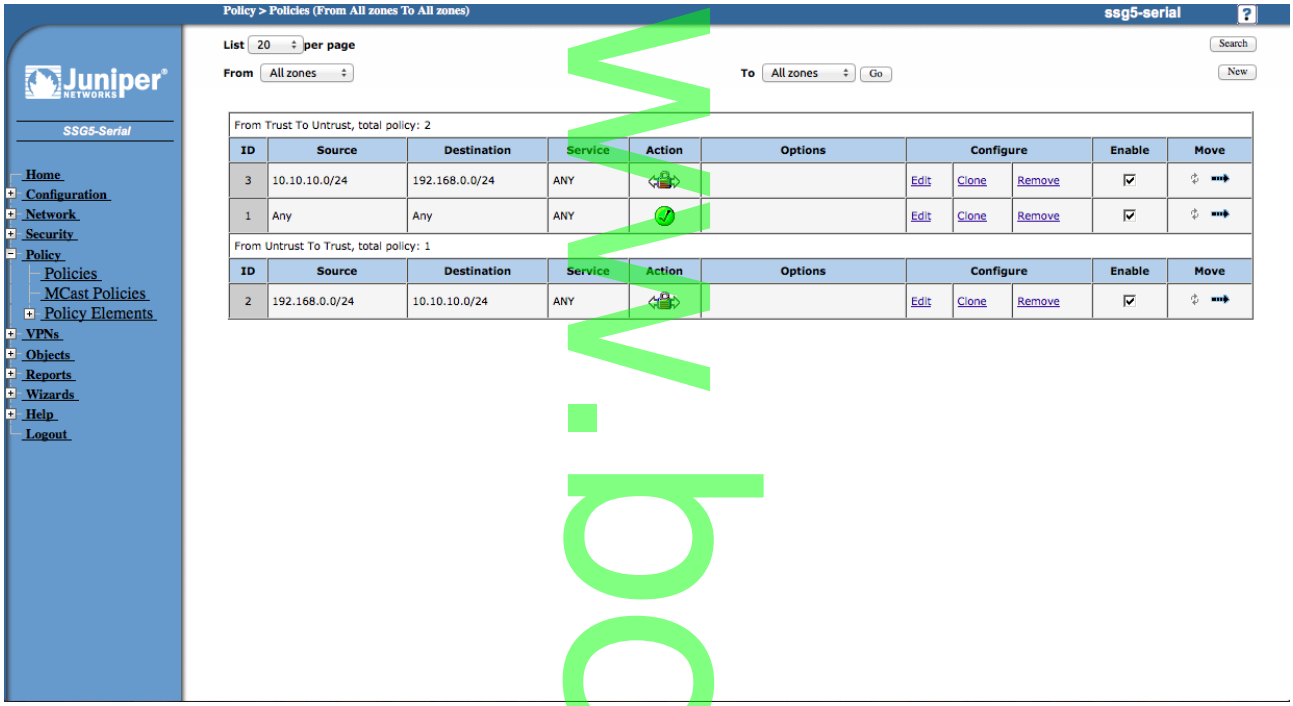


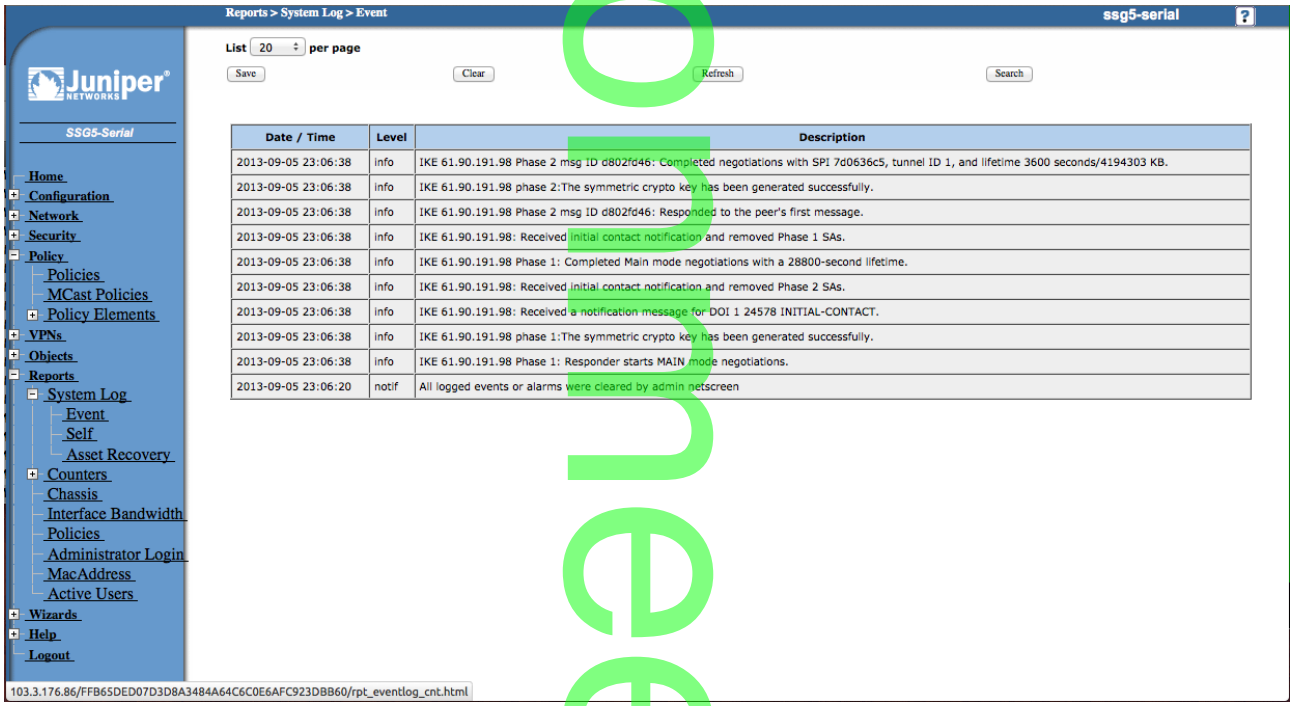



VPNs > AutoKey IKE > Edit
ssg5-serial
SSG5-Serial
Home
Configuration
Network
Binding
DNS
Zones
Interfaces
List
Backup
DHCP
802.1X
Routing
PPP
Security
Policy
VPNs
AutoKey IKE
AutoKey Advanced
Gateway
P1 Proposal
P2 Proposal
XAuth Settings
VPN Groups
Manual Key
L2TP
Monitor Status
Security Level
Predefined
Standard
Compatible
Basic
User Defined
Custom
Phase 2 Proposal
nopfs-esp-3des-md5
None
None
None
Replay Protection
Transport Mode
Bind to
None
Tunnel Interface
Tunnel Zone
none
Untrust-Tun
Proxy-ID
Local IP / Netmask
Remote IP / Netmask
Service
ANY
DSCP Marking
Disable
Enable
Dscp Value
VPN Group
None
Weight
VPN Monitor
Source Interface
default
Destination IP
default
Optimized
Rekey
Return
Cancel


Policy > Policies (From Trust To Untrust)
ssg5-serial
SSG5-Serial
Home
Configuration
Network
Security
Policy
Policies
MCast Policies
Policy Elements
VPNs
Objects
Reports
Wizards
Help
Logout
Name (optional)
192.168.0.0
Source Address
New Address
Address Book Entry
10.10.10.0/24
Multiple
Destination Address
New Address
Address Book Entry
192.168.0.0/24
Multiple
Service
ANY
Multiple
Application
None
WEB Filtering
Action
Tunnel
Deep Inspection
Tunnel
VPN
VPN1
Modify matching bidirectional VPN policy
L2TP
None
Logging
at Session Beginning
Session-limit
Counter
0
Alarm without drop
OK
Cancel
Advanced


Policy > Policies (From Untrust To Trust)
ssg5-serial
SSG5-Serial
Home
Configuration
Network
Security
Policy
Policies
MCast Policies
Policy Elements
VPNs
Objects
Reports
Wizards
Help
Logout
Name (optional)
192.168.0.0
Source Address
New Address
Address Book Entry
192.168.0.0/24
Multiple
Destination Address
New Address
Address Book Entry
10.10.10.0/24
Multiple
Service
ANY
Multiple
Application
None
WEB Filtering
Action
Tunnel
Deep Inspection
Tunnel
VPN
VPN1
Modify matching bidirectional VPN policy
L2TP
None
Logging
at Session Beginning
Session-limit
Counter
0
Alarm without drop
OK
Cancel
Advanced





[Cisco]
ip access-list extended VPN
 permit ip 192.168.0.0 0.0.0.255 10.10.10.0 0.0.0.255

crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 112233 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set JUNIPER-SSG5 esp-3des esp-md5-hmac
crypto map JUNIPER-SSG5 10 ipsec-isakmp
 set peer 103.3.176.86
 set transform-set JUNIPER-SSG5
 match address VPN

 interfae vlan10
          description ## Internet ##
           ip address 61.90.191.98 255.255.255.252
           crypto map JUNIPER-SSG5

Cisco#sh crypto ipsec sa

interface: Vlan10
    Crypto map tag: JUNIPER-SSG5, local addr 61.90.191.98

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 103.3.176.86 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

local crypto endpt.: 61.90.191.98, remote crypto endpt.: 103.3.176.86
path mtu 1500, ip mtu 1500
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

```
Cisco#ping 10.10.10.1 source lo200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/5/8 ms
Cisco#sh crypto ipsec sa

interface: Vlan10
    Crypto map tag: JUNIPER-SSG5, local addr 61.90.191.98

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 103.3.176.86 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
```

local crypto endpt.: 61.90.191.98, remote crypto endpt.: 103.3.176.86

path mtu 1500, ip mtu 1500
current outbound spi: 0x7D0636C5(2097559237)

inbound esp sas:
 spi: 0x123D8D58(306023768)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 15, flow_id: C87X_MBRD:15, crypto map: JUNIPER-SSG5
   sa timing: remaining key lifetime (k/sec): (4392926/3595)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x7D0636C5(2097559237)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 16, flow_id: C87X_MBRD:16, crypto map: JUNIPER-SSG5
   sa timing: remaining key lifetime (k/sec): (4392926/3595)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

outbound ah sas:

outbound pcp sas: