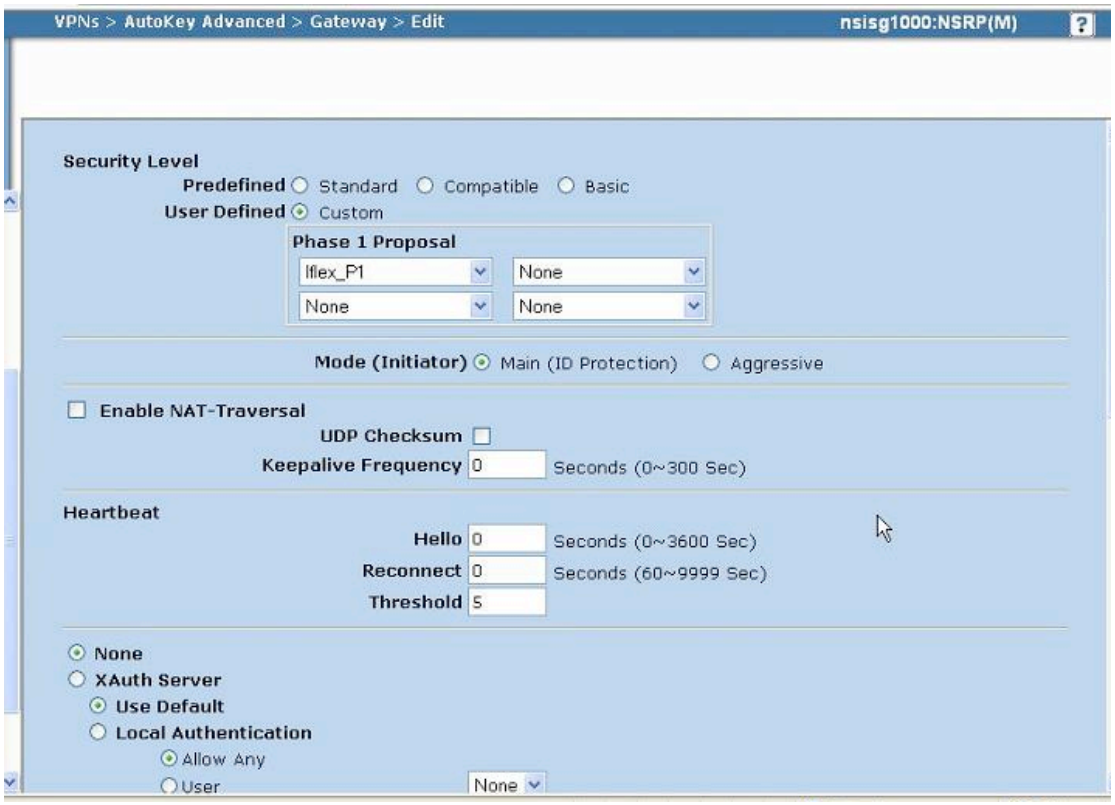
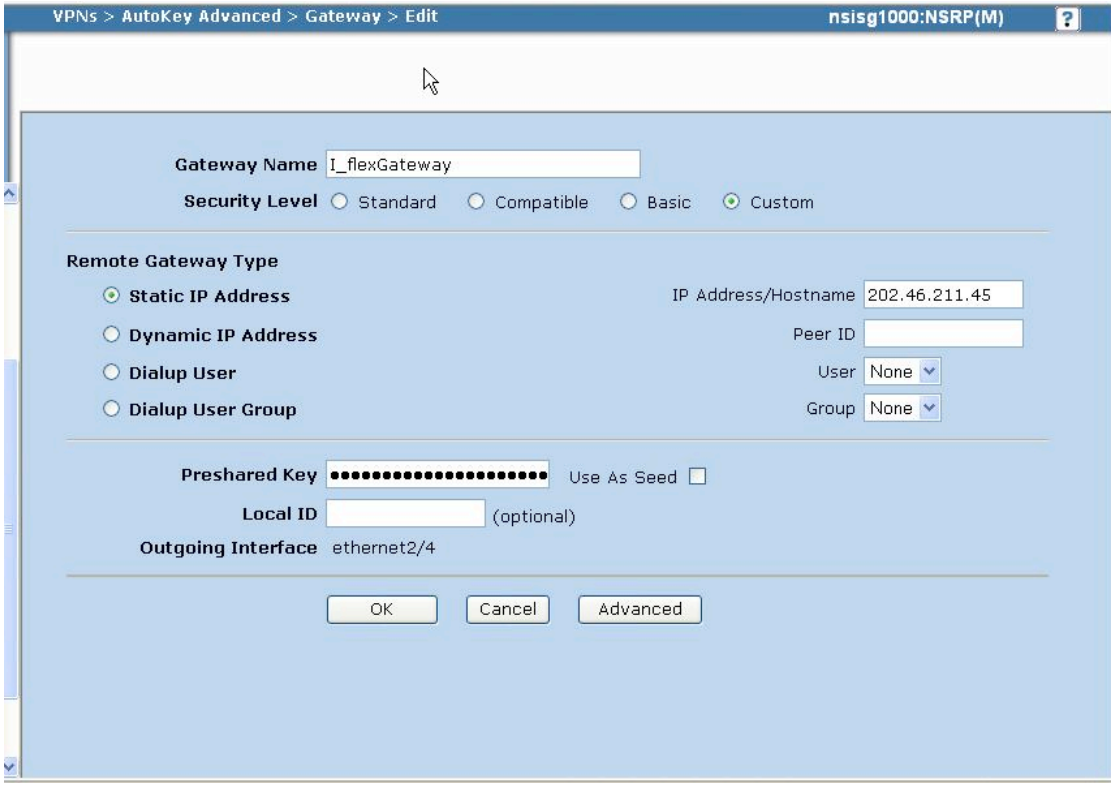
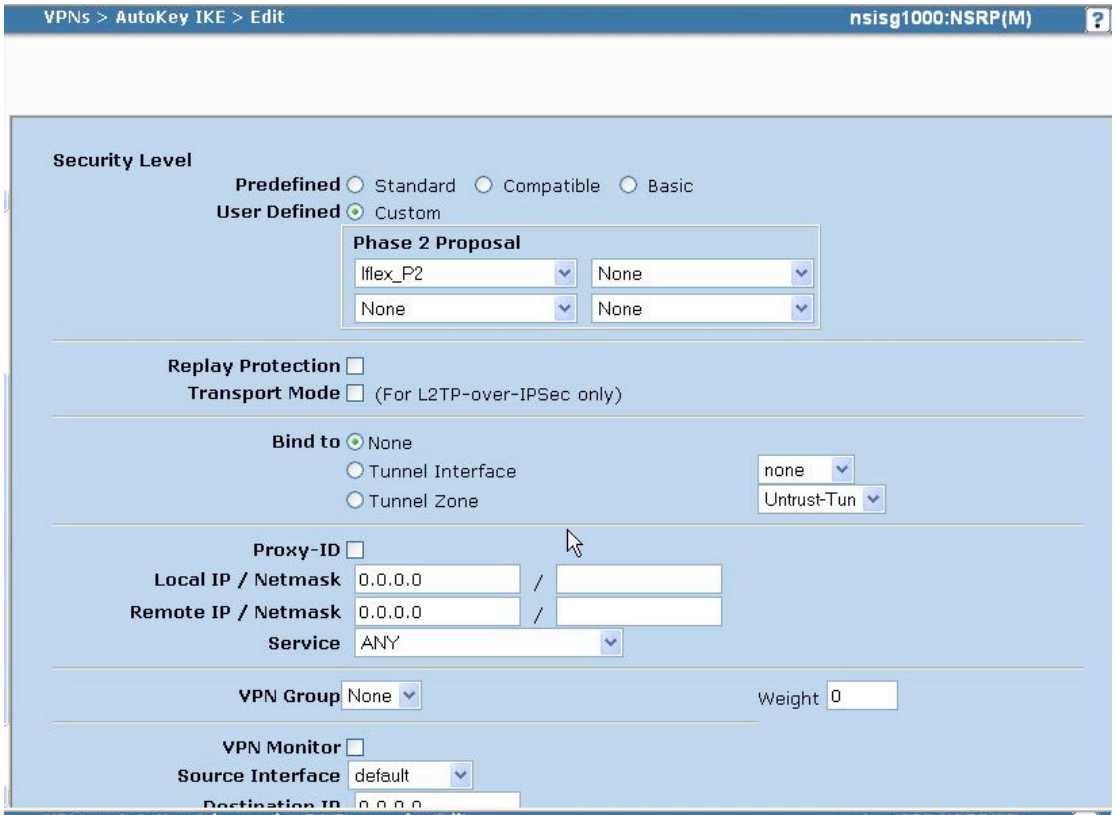
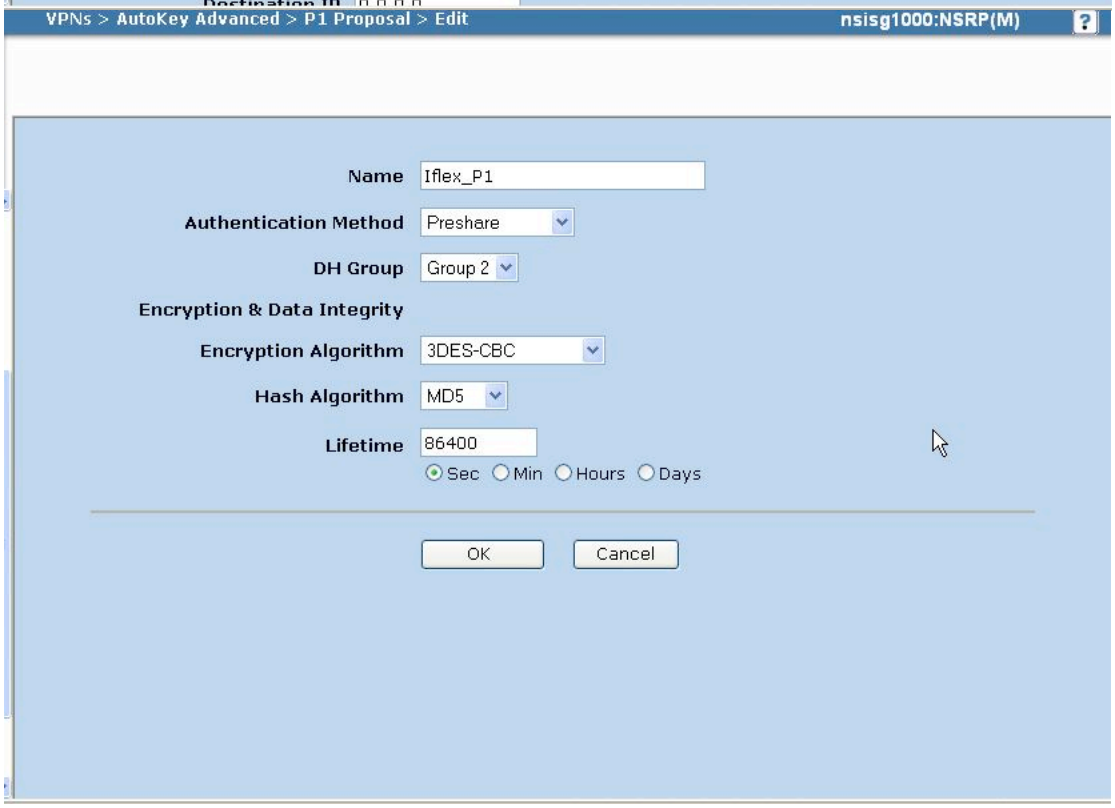
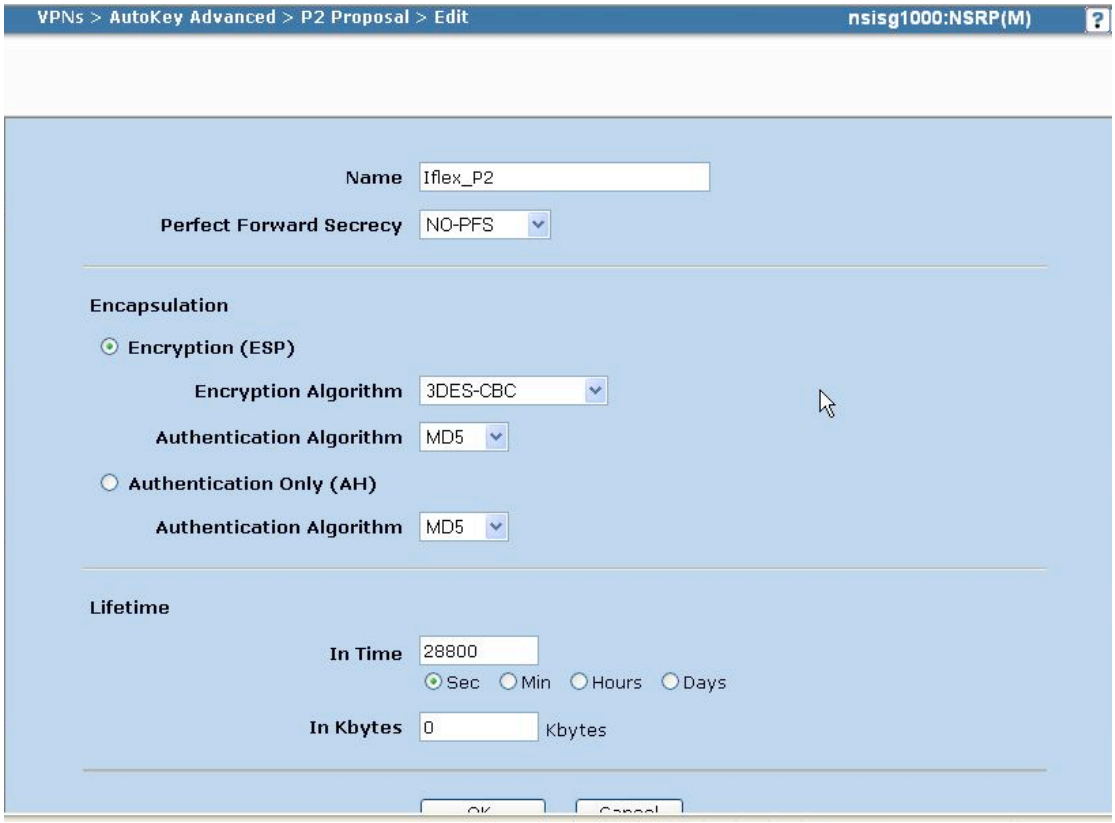
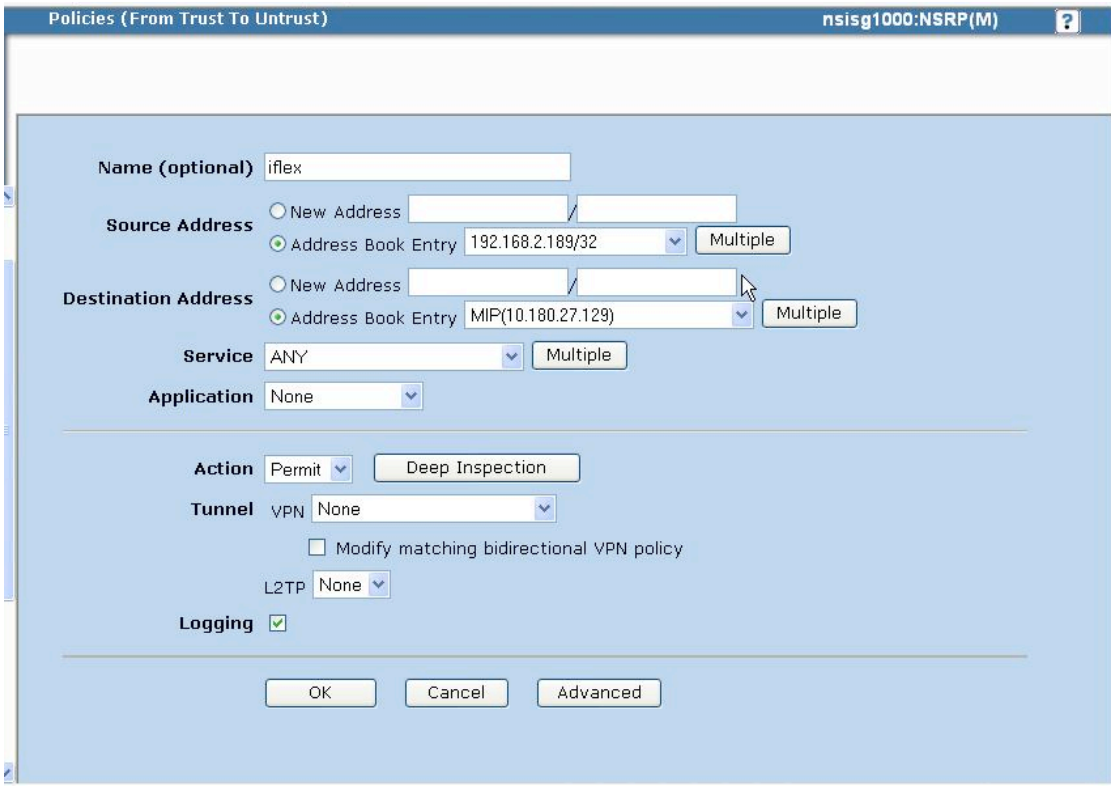

VPNs > AutoKey Advanced > Gateway > Edit
nsisg1000:NSRP(M)
Security Level
Predefined
Standard
Compatible
Basic
User Defined
Custom
Phase 1 Proposal
Iflex_P1
None
None
None
Mode (Initiator)
Main (ID Protection)
Aggressive
Enable NAT-Traversal
UDP Checksum
Keepalive Frequency
0
Seconds (0~300 Sec)
Heartbeat
Hello
0
Seconds (0~3600 Sec)
Reconnect
0
Seconds (60~9999 Sec)
Threshold
5
None
XAuth Server
Use Default
Local Authentication
Allow Any
User
None

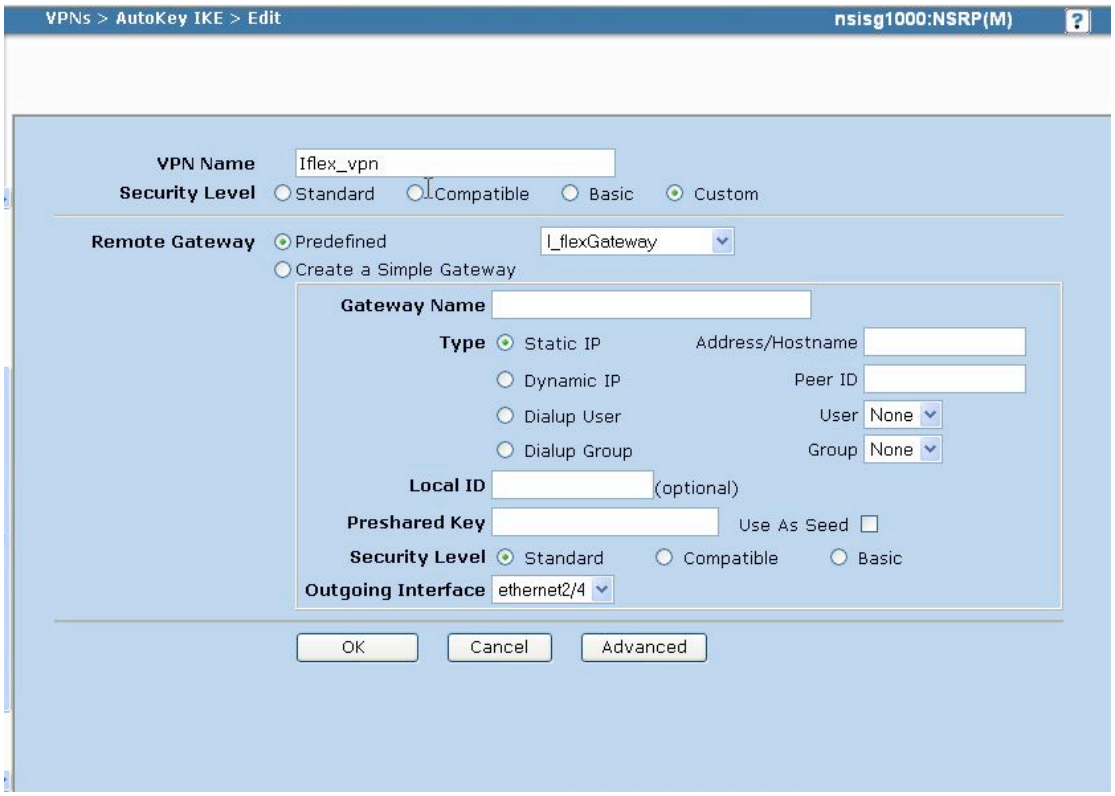

VPNs > AutoKey Advanced > Gateway > Edit
nsisg1000:NSRP(M)
Gateway Name
I_flexGateway
Security Level
Standard
Compatible
Basic
Custom
Remote Gateway Type
Static IP Address
Dynamic IP Address
Dialup User
Dialup User Group
IP Address/Hostname
202.46.211.45
Peer ID
User
None
Group
None
Preshared Key
Use As Seed
Local ID
(optional)
Outgoing Interface
ethernet2/4
OK
Cancel
Advanced

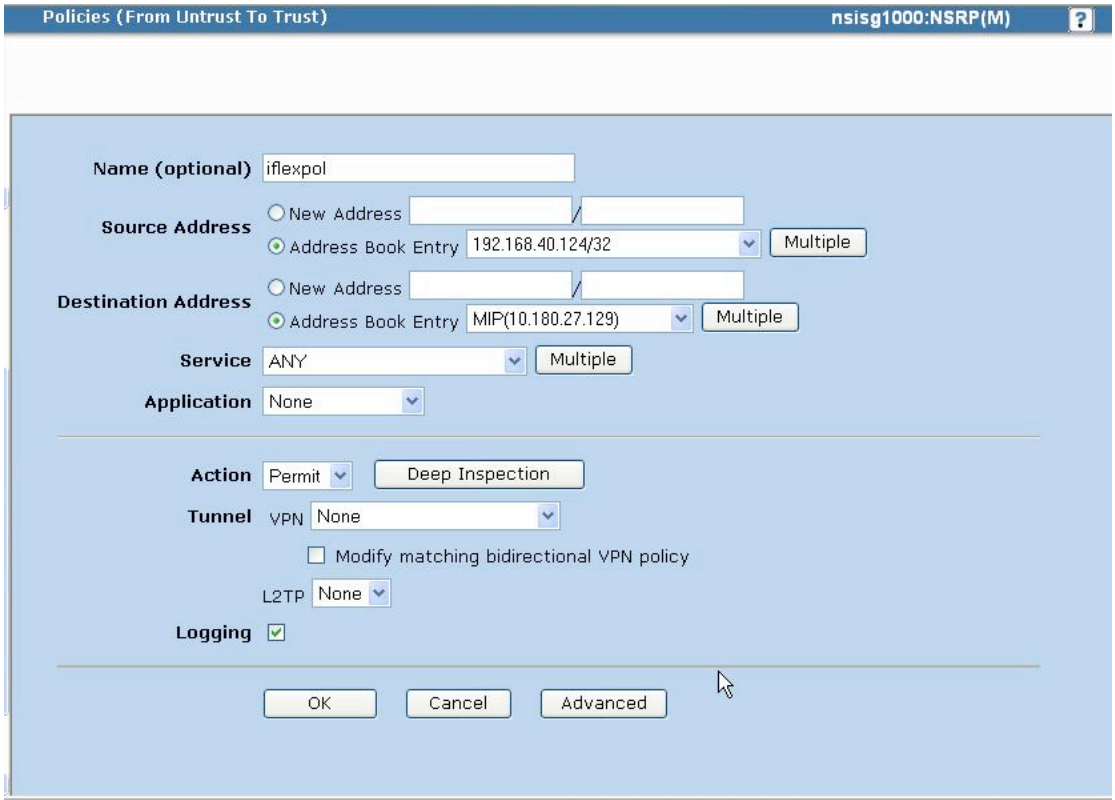

VPNs > AutoKey IKE > Edit
nsisg1000:NSRP(M)
Security Level
Predefined
Standard
Compatible
Basic
User Defined
Custom
Phase 2 Proposal
Iflex_P2
None
None
None
Replay Protection
Transport Mode
(For L2TP-over-IPSec only)
Bind to
None
Tunnel Interface
none
Tunnel Zone
Untrust-Tun
Proxy-ID
Local IP / Netmask
0.0.0.0
Remote IP / Netmask
0.0.0.0
Service
ANY
VPN Group
None
Weight
0
VPN Monitor
Source Interface
default

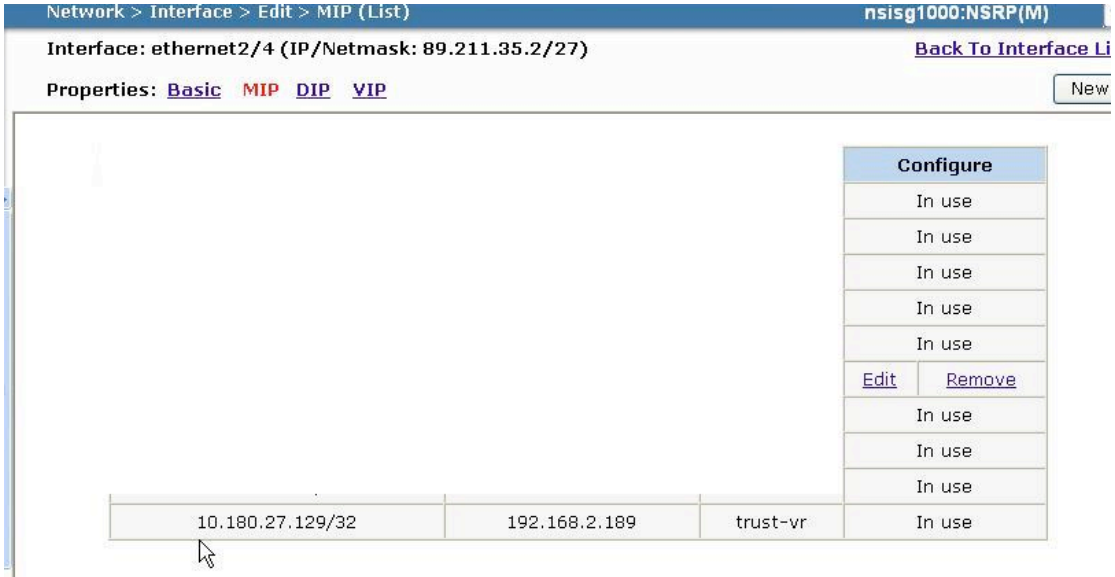

VPNs > AutoKey Advanced > P1 Proposal > Edit
nsisg1000:NSRP(M)
Name
Iflex_P1
Authentication Method
Preshare
DH Group
Group 2
Encryption & Data Integrity
Encryption Algorithm
3DES-CBC
Hash Algorithm
MD5
Lifetime
86400
Sec
Min
Hours
Days
OK
Cancel

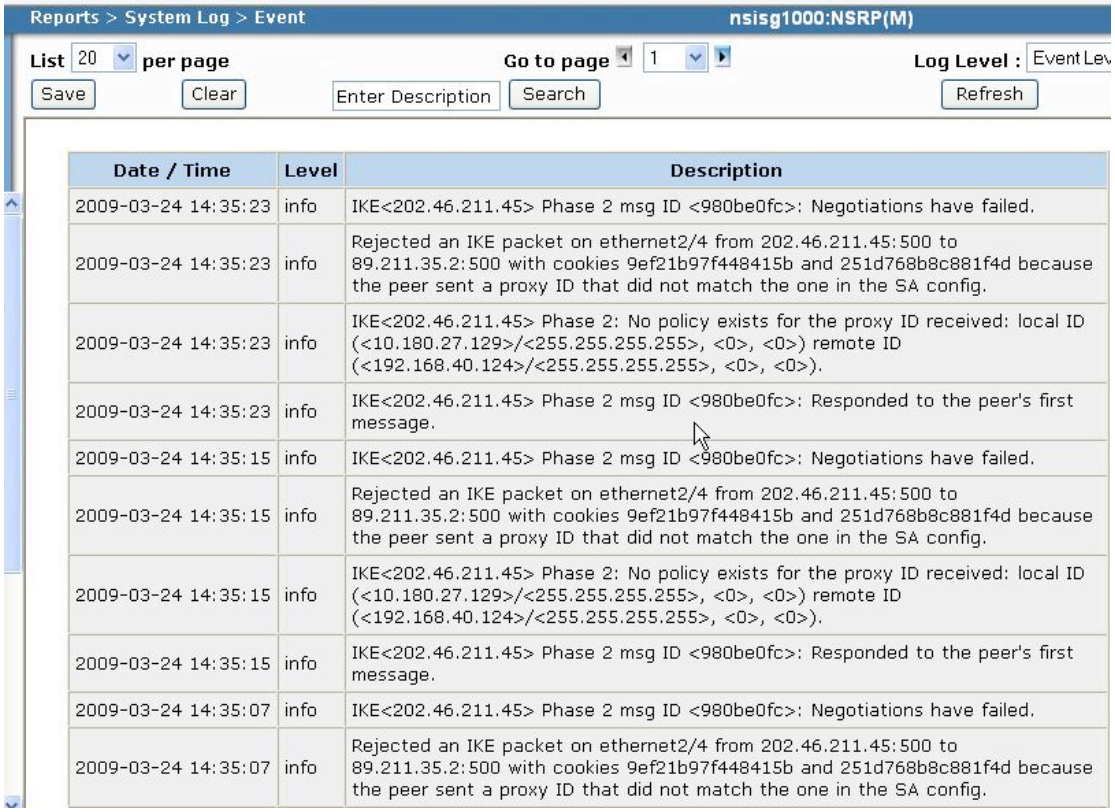

VPNs > AutoKey Advanced > P2 Proposal > Edit
nsisg1000:NSRP(M)
Name
Iflex_P2
Perfect Forward Secrecy
NO-PFS
Encapsulation
Encryption (ESP)
Encryption Algorithm
3DES-CBC
Authentication Algorithm
MD5
Authentication Only (AH)
Authentication Algorithm
MD5
Lifetime
In Time
28800
Sec
Min
Hours
Days
In Kbytes
0
Kbytes


Policies (From Trust To Untrust)
nsisg1000:NSRP(M)
Name (optional)
iflex
Source Address
New Address
Address Book Entry
192.168.2.189/32
Multiple
Destination Address
New Address
Address Book Entry
MIP(10.180.27.129)
Multiple
Service
ANY
Multiple
Application
None
Action
Permit
Deep Inspection
Tunnel
VPN
None
Modify matching bidirectional VPN policy
L2TP
None
Logging
OK
Cancel
Advanced


VPNs > AutoKey IKE > Edit
nsisg1000:NSRP(M)
VPN Name
Iflex_vpn
Security Level
Standard
Compatible
Basic
Custom
Remote Gateway
Predefined
I_flexGateway
Create a Simple Gateway
Gateway Name
Type
Static IP
Address/Hostname
Dynamic IP
Peer ID
Dialup User
User
None
Dialup Group
Group
None
Local ID
(optional)
Preshared Key
Use As Seed
Security Level
Standard
Compatible
Basic
Outgoing Interface
ethernet2/4
OK
Cancel
Advanced


Policies (From Untrust To Trust)
nsisg1000:NSRP(M)
Name (optional)
iflexpol
Source Address
New Address
Address Book Entry
192.168.40.124/32
Multiple
Destination Address
New Address
Address Book Entry
MIP(10.180.27.129)
Multiple
Service
ANY
Multiple
Application
None
Action
Permit
Deep Inspection
Tunnel
VPN
None
Modify matching bidirectional VPN policy
L2TP
None
Logging
OK
Cancel
Advanced





Date / Time	Level	Description
2009-03-24 14:35:23	info	IKE<202.46.211.45> Phase 2 msg ID <980be0fc>: Negotiations have failed.
2009-03-24 14:35:23	info	Rejected an IKE packet on ethernet2/4 from 202.46.211.45:500 to 89.211.35.2:500 with cookies 9ef21b97f448415b and 251d768b8c881f4d because the peer sent a proxy ID that did not match the one in the SA config.
2009-03-24 14:35:23	info	IKE<202.46.211.45> Phase 2: No policy exists for the proxy ID received: local ID (<10.180.27.129>/<255.255.255.255>, <0>, <0>) remote ID (<192.168.40.124>/<255.255.255.255>, <0>, <0>).
2009-03-24 14:35:23	info	IKE<202.46.211.45> Phase 2 msg ID <980be0fc>: Responded to the peer's first message.
2009-03-24 14:35:15	info	IKE<202.46.211.45> Phase 2 msg ID <980be0fc>: Negotiations have failed.
2009-03-24 14:35:15	info	Rejected an IKE packet on ethernet2/4 from 202.46.211.45:500 to 89.211.35.2:500 with cookies 9ef21b97f448415b and 251d768b8c881f4d because the peer sent a proxy ID that did not match the one in the SA config.
2009-03-24 14:35:15	info	IKE<202.46.211.45> Phase 2: No policy exists for the proxy ID received: local ID (<10.180.27.129>/<255.255.255.255>, <0>, <0>) remote ID (<192.168.40.124>/<255.255.255.255>, <0>, <0>).
2009-03-24 14:35:15	info	IKE<202.46.211.45> Phase 2 msg ID <980be0fc>: Responded to the peer's first message.
2009-03-24 14:35:07	info	IKE<202.46.211.45> Phase 2 msg ID <980be0fc>: Negotiations have failed.
2009-03-24 14:35:07	info	Rejected an IKE packet on ethernet2/4 from 202.46.211.45:500 to 89.211.35.2:500 with cookies 9ef21b97f448415b and 251d768b8c881f4d because the peer sent a proxy ID that did not match the one in the SA config.