RV016, RV042, RV042G ë°© RV082 VPN ë©¼ìš°í„°ì—©ì„œ VPN í©´ë©¼ì©´ì–¸íŠ¸ì—© ëŒ€í•œ ì›©ê²© ì•¡ì„¸ìŠ¤ í„°ë„©(í©´ë©¼ì©´ì–¸íŠ¸-ê²Œì©´íŠ¸ì›¨ì©´) ì„¤ì •

ëª©í‘œ

ì©´ ë¬¸ì„œì—©ì„œëŠ” RV016, RV042, RV042G ë°© RV082 VPN ë©¼ìš°í„°ì—©ì„œ The Green Bow ë˜©ëŠ” VPN Trackerì™€ ê°™ì©´ ì„œë“œëŒŒí‹° VPN í©´ë©¼ì©´ì–¸íŠ¸ ì†Œí”„íŠ¸ì¨ì–´ë¥¼ ì‚¬ìš©í•˜ì—¬ í©´ë©¼ì©´ì–¸íŠ¸ì—©ì„œ ê²Œì©´íŠ¸ì›¨ì©´ë¡œ ì©¡ì„¸ìŠ¤ VPN(Virtual Private Network) í„°ë„©ì©„ êµ¬ì„±í•˜ëŠ” ë°©ë²•ì—© ëŒ€í•´ ì„¤ëª…í•©ë‹ˆë‹¤.

ì†Œê°œ

VPNì©€ ê³µìš© ë„¤íŠ¸ì›Œí©¬ë¥¼ í†µí•´ ì›©ê²© ì‚¬ìš©ìž©ì¹˜ì©¼ ìž¥ì¹˜ë¥¼ ê°€ìƒ©ì—©ì„œ ì—°ê²°í•˜ì—¬ ë‚´ œê³µí•˜ëŠ” ë°° ì‚¬ìš©ë•˜ëŠ” ì‚¬ìš©ìž…ë‹ˆë‹¤. ì›©ê²© ì•¡ì„¸ìŠ¤ í„°ë„©ì©„ VPNì©€ í©´ë©¼ì©´ì–¸íŠ¸ ì»´í“¨í„°ì™€ ë„¤íŠ¸ì›Œí©¬ ê°„ì—© VPNì©„ êµ¬ì„±í•˜ëŠ” ë°° ì‚¬ìš©ë•˜ëŠ” í„°ë„œì„œ ìŠ¤ìž…ë‹ˆë‹¤. í©´ë©¼ì©´ì–¸íŠ¸ ë°°ìŠ¤í©¬ë¡œ VPN í©´ë©¼ì©´ì–¸íŠ¸ ì†Œí”„íŠ¸ì¨ì–´ë¥¼ í•©ë¡œ ì‚¬ìš©ì©€ ì›©ê²©©ì¼ë¡œ ì•ˆ „í•˜ê²Œ ë„¤íŠ¸ì›Œí©¬ì—© ì—°ê²°í• ìˆ˜ ìžˆë©„ë©„ ìš©ì›©í©¬ë¡œ ì•ˆ „í•˜ê²Œ ì—°ê²°í•˜ëŠ” ë°© ìœ©ì›©ì©€ ì„¤ëª…í•©ë‹ˆë‹¤.

ì ìš© ê°€ëŠ¥í•œ ìž¥ì¹˜

- RV016
- RV042
- RV042G
- RV082

ì†Œí”„íŠ¸ì¨ì–´ ë²„ì „

- v4.2.2.08

VPN í„°ë„© êµ¬ì„±

1ë‹¨ê³„. ì›¹ ì»´í”¼ê·¸ë ˆì´...˜ ìœ í‹¸ë¦¬í‹°ì—© ë¡œê·¸ì©¸í•©ë‹ˆë‹¤. **VPN > Client to Gatewayë¥¼ ì„ íƒ©í•©ë‹ˆë‹¤.** í©´ë©¼ì©´ì–¸íŠ¸ *ëŒ€ ê²Œì©´íŠ¸ì›¨ì©´ íŽ˜ì©€ê°€ ì—´ë¦½ë‹ˆë‹¤.

ìƒˆ í„°ë„ ì¶”ê°€

1ë‹¨ê³„. ì¶”ê°€í•˜ë ¤ëŠ” í„°ë„ ì¢…ë¥˜ ë”°ë¼ ì ˆí•œ ë²„íŠ¼ì„ ëˆ„ë¦…ë‹ˆë‹¤.

- Tunnel - ì›ê²© ë‹¨ì¼ ì‚¬ìš©ìž ê¸°ë°˜ ëŒ€í•œ í„°ë„ ë‚˜íƒ€ëƒ…ë‹¤.
- Group VPN(ê·¸ë£¹ VPN) - ì›ê²© ì‚¬ìš©ìž ê·¸ë£¹ì˜ í„°ë„ ë‚˜íƒ€ëƒ…ë‹¤.

Tunnel Number(í„°ë„ë²ˆí˜¸)ëŠ” í„°ë„ ë²ˆí˜¸ë¥¼ í‘œì‹œí•˜ëŠ” ìž„ì‹œë¡œ ìƒ‰ì„ í•„ìš”ë…„ë‹¤.

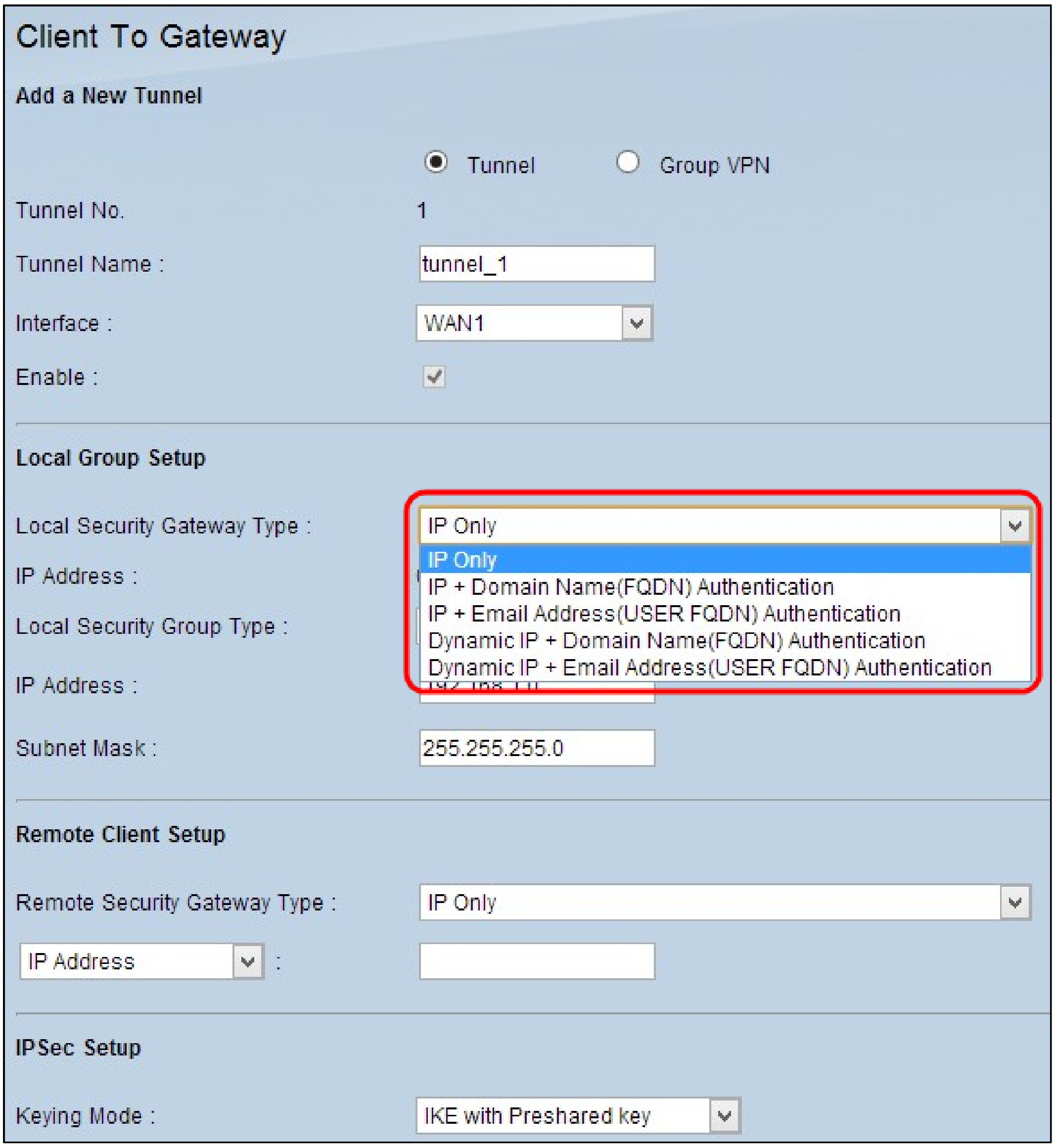
2ë‹¨ê³„. Tunnel Name(í„°ë„ ì´ë¦„) í•„ë“œì—ì„œ í„°ë„ ì´ë¦„ì„ ìž…ë ¥í•©ë‹¤.

3ë‹¨ê³„. Interface ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ VPN í„°ë„ì—ì„œ ì‚¬ìš©í• ì „ì²´ WAN ì¸í„°íŽ˜ì´ìŠ¤ë¥¼ ì„ íƒí•©ë‹¤.

4ë‹¨ê³„. (ì„ íƒ ì‚¬í•) VPNì„ ì™„ì „ížˆ ë¹„í™œì„±í™”í•˜ë ¤ë©´ Enable(í™œì„±í™”) í•„ë“œì—ì„œ í™•ì¸ëž€ì„ ì„ íƒí•©ë‹¤. ê¸°ë³¸ ì¤ì´ ìžˆìµë‹¤.

ë¡œì»¬ ê·¸ë£¹ ì„¤ì •

1ë‹¨ê³„. *Local Security* Gateway ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ VPN í„°ë„ì—ì„œ ì„¤ì •í•œ ì „ì²´ ì‹ë³„ìžë¥¼ ì ˆí•œ ë¼ìš°í„° ì‹¤ë³„ ë°©ë²•ì„ ì„ íƒí•©ë‹¤. *Add A New Tunnel(ìƒˆ í„°ë„ ì¶”ê°€)* ì„¤ì •ì—ì„œ 1ë‹¨ê³„ì—ì„œ Group VPN(ê·¸ë£¹ VPN)ì„ ì„ íƒí•œ ê²½ìš° ì´ *ë‹¨ê³„ë¥¼* ê±´ë„ˆëœ€ë‹¤.



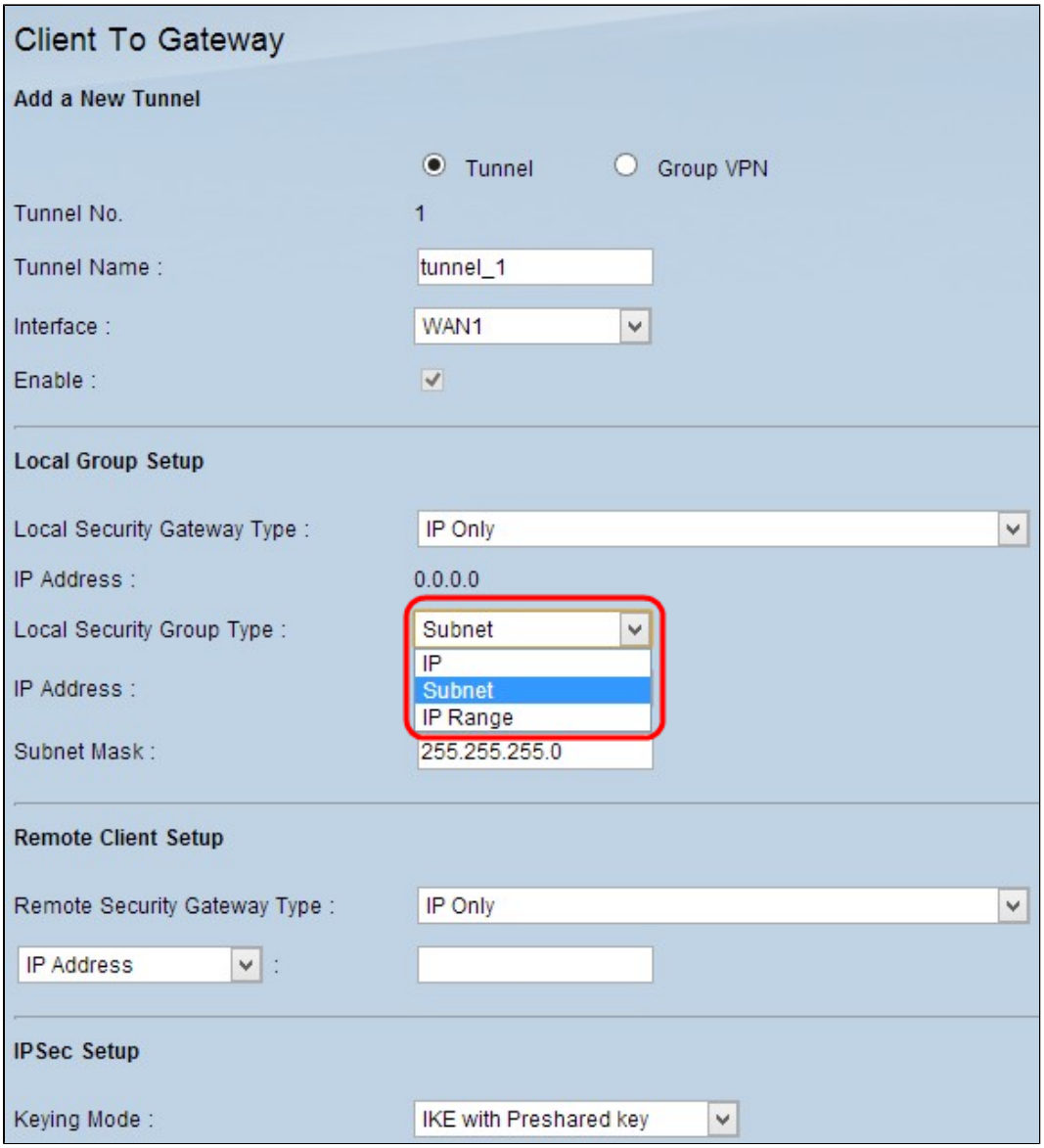
- IP Only(IP ì „ìš©) - ê³ ì • WAN IP ì£¼ì†Œë¥¼ í†µí•´ í„°ë„„ì— ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆìŠµë‹ˆë‹¤. ë¼ìš°í„°ì— ê³ ì • WAN IPê°€ ìžˆëŠ” ê²½ìš°ì—ë§Œ ì´ ì˜µì…˜ì„ ì„ íƒí• ìˆ˜ ìžˆìŠµë‹ˆë‹¤. ê³ ì • WAN IP ì£¼ì†Œê°€ ìžë™ìœ¼ë¡œ ë‚˜íƒ€ë‚©ë‹ˆë‹¤.
- IP + ë„ë©”ì¸ ì´ë¦„(FQDN) ì¸ì¦ - ê³ ì • IP ì£¼ì†Œ ë°ë“±ë¡ë œ FQDN (Fully Qualified Domain Name) ë„ë©”ì¸ì„ í†µí•´ í„°ë„„ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆìŠµë‹ˆë‹¤. ê³ ì • WAN IP ì£¼ì†ŒëŠ” ìžë™ìœ¼ë¡œ ìƒì„±ë©ë‹ˆë‹¤.
- IP + ì´ë©”ì¼ ì£¼ì†Œ(ì‚¬ìš©ìž FQDN) ì¸ì¦ - ê³ ì • IP ì£¼ì†Œì™€ ì´ë©”ì¼ ì£¼ì†Œë¥¼ í†µí•´ í„°ë„„ì— ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆìŠµë‹ˆë‹¤. ê³ ì • WAN IP ì£¼ì†ŒëŠ” ìžë™ìœ¼ë¡œ ìƒì„±ë©ë‹ˆë‹¤.
- ë™ì IP + FQDN(Domain Name) ì¸ì¦ - ë™ì IP ì£¼ì†Œ ë°ë“±ë¡ëœ ë„ë©”ì¸ì„ í†µí•´ í„°ë„„ì— ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆìŠµë‹ˆë‹¤.
- ë™ì IP + ì´ë©”ì¼ ì£¼ì†Œ(ì‚¬ìš©ìž FQDN) ì¸ì¦ â€” ë™ì IP ì£¼ì†Œ ë°ì´ë©”ì¼ ì£¼ì†Œë¥¼ í†µí•´ í„°ë„„ì— ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆìŠµë‹ˆë‹¤.

2ë‹¨ê³„. 1ë‹¨ê³„ì—ì„œ *IP + FQDN(Domain Name) ì¸ì¦ ë˜ëŠ” ë™ì IP + FQDN(Domain Name) ì¸ì¦*ì„ ì„ íƒí•œ ê²½ìš° ë“±ë¡ëœ FQDN(Fully Qualified Domain)ì˜ ì´ë¦„ì„ Domain Name í•„ë“œì— ìž…ë ¥í•©ë‹ˆë‹¤.

3ë‹¨ê³„. 1ë‹¨ê³„ì—ì„œ *IP + E-mail Address(USER FQDN) Authentication(IP + E-mail Address(USER FQDN) ì¸ì¦)* ë˜ëŠ” *Dynamic IP + E-mail Address(USER FQDN) Authentication(ë™ì IP + E-mail ì£¼ì†Œ(USER FQDN) ì¸ì¦)*ì„ ì„ íƒí•œ ê²½ìš° Email Address(ì´ë©”ì¼ ì£¼ì†Œ) í•„ë“œì— ì´ë©”ì¼ ì£¼ì†Œë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤.

4ë‹¨ê³„. Local *Security Group* ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ VPN í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ì^˜ ìž^ëŠ” ì ì^í•œ ë¡œì»¬ LAN ì‚¬ìš©ìž ë˜ëŠ” ì‚¬ìš©ìž ê·¸ë£¹ì„ ì„ íƒí•©ë‹ˆë‹¤.

- IP - íŠ¹ì • LAN ë””ë°”ì´ìŠ¤ í•˜ë‚˜ë§Œ í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ì^˜ ìž^ìŠµë‹^ë‹¤. ì´ ì˜µì…˜ì„ ì„ íƒí•˜ëŠ” ê²½ìš° IP Address(IP ì£¼ì†Œ) í•„ë“œì—ì„œ LAN ë””ë°”ì´ìŠ¤ì˜ IP ì£¼ì†Œë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤. ê¸°ë³¸ IPëŠ” 192.168.1.0ìž…ë‹^ë‹¤.
- ì„œë¸Œë„· - íŠ¹ì • ì„œë¸Œë„·ì—ì„œ ëª¨ë“ LAN ë””ë°”ì´ìŠ¤ê°€ í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ì^˜ ìž^ìŠµë‹^ë‹¤. ì´ ì˜µì…˜ì„ ì„ íƒí•˜ëŠ” ê²½ìš° IP Address(IP ì£¼ì†Œ) ë°• Subnet Mask(ì„œë¸Œë„· ë§ˆìŠ¤í¬) í•„ë“œì—ì„œ LAN ë””ë°”ì´ìŠ¤ì˜ IP ì£¼ì†Œì™€ ì„œë¸Œë„· ë§ˆìŠ¤í¬ë¥¼ ê°•ê° ìž…ë ¥í•©ë‹ˆë‹¤. ê¸°ë³¸ ë§ˆìŠ¤í¬ëŠ” 255.255.255.0ìž…ë‹^ë‹¤.
- IP Range(IP ë²”ìœ„) - í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ì^˜ ìž^ëŠ” LAN ë””ë°”ì´ìŠ¤ì˜ ë²”ìœ„ë„ìž…ë‹^ë‹¤. ì´ ì˜µì…˜ì„ ì„ íƒí•˜ëŠ” ê²½ìš° Begin IP(ì‹œìž‘ IP) ë°• End IP(ì¢…ë£Œ IP) í•„ë“œì—ì„œ ê°•ê° ì‹œìž‘ ë°• ì¢…ë£Œ IP ì£¼ì†Œë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤. ê¸°ë³¸ ë²”ìœ„ëŠ” 192.168.1.0~192.168.1.254ìž…ë‹^ë‹¤.

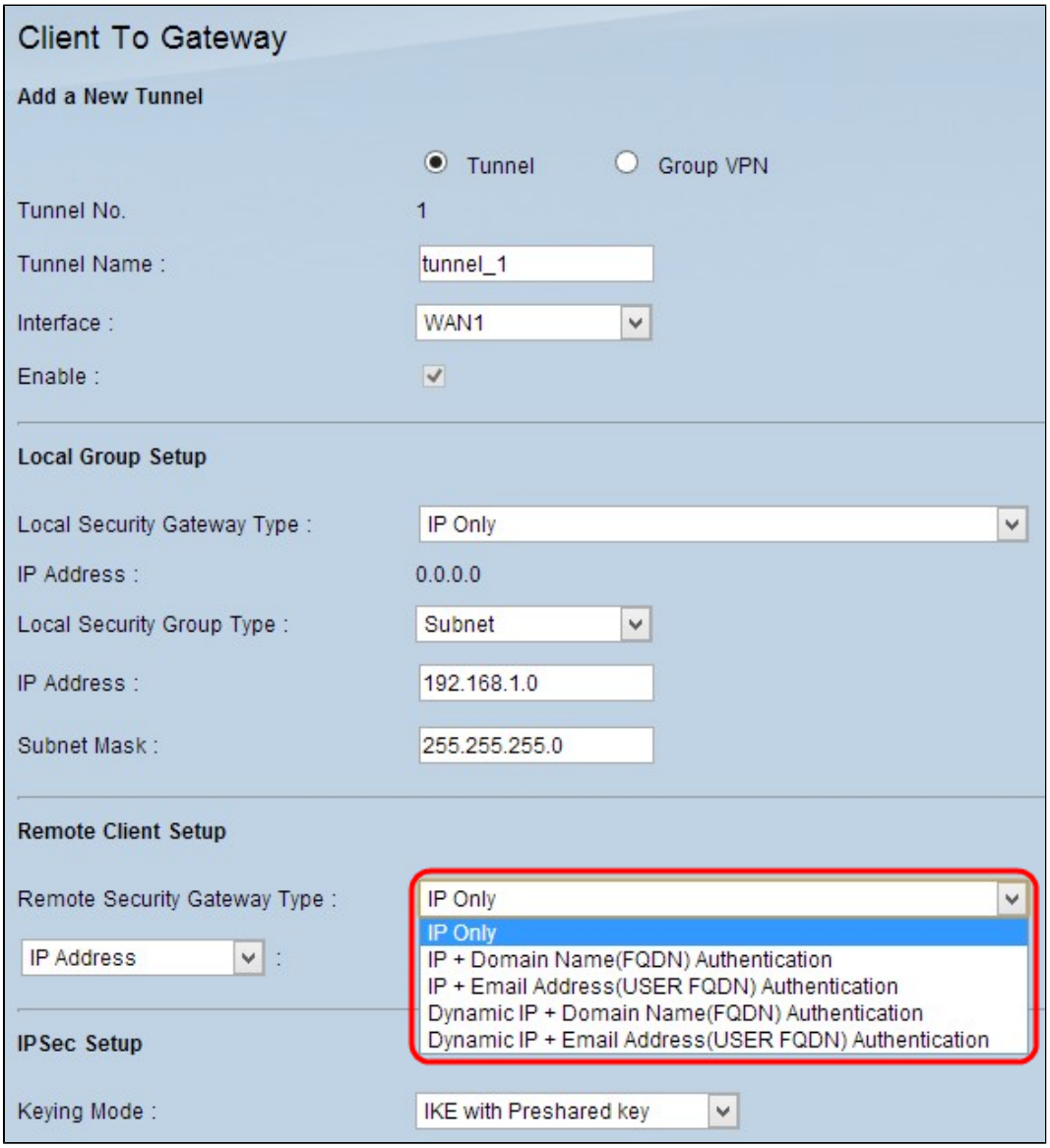


5ë‹¨ê³„. Save(**ì €ìž¥**)ë¥¼ í´ë¦í•˜ì—¬ ì„¤ì •ì„ ì €ìž¥í•©ë‹ˆë‹¤.

ì›ê²© í´ë¼ì´ì–¸íŠ¸ ì„¤ì •

1ë‹¨ê³„. Tunnel(í„°ë„)ì„ ì„ íƒí•œ ê²½ìš° *Remote Security Gateway Type(ì›ê²© ë³´ì•ˆ

ê²Œì�´íŠ¸ì› ¨ì�´ìœ í˜•) ë“œë¡ë‹¤ìš´ ëª©ë¡�ì—�ì„œ VPN í„°ë„�ì�„ ì„¤ì •í•˜ëŠ” ì €ì•¤ì�´ì–¸íŠ¸ ì‹œë³„ ë°©ë²•ì•„ë„ ì„ íƒ•©ë‹ˆë‹¤. ê¸°ë³¸ê°’ì€ IP Only(IP ì „ìš©)ìž…ë‹¤. *Add A New Tunnel(ì†ˆí„°ë„ ì¶”ê°€) ì„ ì„ íƒ•œ ë’¤ 1ë‹¨ê³„ì—�ì„œ Group VPN(ê·¸ë£¹ VPN)ì�„ ì„ íƒ•œ ê²½ìš° ì�´ ë‹¨ê³„ë¥¼ ê±´ë„ˆëœ€ë‹ˆë‹¤.*



- IP Only(IP ì „ìš©) - í�´ë�¼ì�´ì–¸íŠ¸ì�˜ ê³ ì • WAN IPë¥¼ í†µí•´ì„œë§Œ í„°ë„�ì—�ì„œ ì•¡ì„¸ìŠ¤í• ì ˆì„ ì‹œë„í•©ë‹ˆë‹¤. ì�´ ì˜µì…˜ì�„ ì‚¬ìš©í•˜ë ¤ë©´ í´ë¼ì–¸íŠ¸ì˜ ê³ ì • WAN IPë¥¼ ì•Œì•„ì•¼ í•©ë‹ˆë‹¤.
- IP + ë„„ë©”ì„ ì�´ë¦„ (FQDN) ì„ì¦ - í„°ë„�ì—�ë Œ€í•œ ì•¡ì„¸ìŠ¤ëŠ” í´ë¼ì–¸íŠ¸ì˜ ê³ ì • IP ì£¼ì†Œ ë°• ë“±ë¡ ë œ ë„„ë©”ì„ì¦ í†µí•´ ê°€ëŠ¥í•©ë‹ˆë‹¤.
- IP + E-mail Address (USER FQDN) Authentication(IP + E-mail ì£¼ì†Œ(ì‚¬ìš©ìž FQDN) ì„ì¦) - í´ë¼ì–¸íŠ¸ì˜ ê³ ì • IP ì£¼ì†Œ™€ ì´ë©”ì¼ ì£¼ì†Œë¥¼ í†µí•´ í„°ë„�ì—�ì•¡ì„¸ìŠ¤í• ì ˆì„ ìž¥ì¹˜ë‹¤.
- Dynamic IP + Domain Name (FQDN) Authentication(ë™ì IP + ë„„ë©”ì„ ì´ë¦„(FQDN) ì„ì¦) - í´ë¼ì–¸íŠ¸ì˜ ë°• ë“±ë¡ë œ ë„„ë©”ì„ì¦ ë™ì IP ì£¼ì†Œë¥¼ í†µí•´ í„°ë„�ì—�ì•¡ì„¸ìŠ¤í• ì ˆì„ ìž¥ì¹˜ë‹¤.
- ë™ì IP + ì´ë©”ì¼ ì£¼ì†Œ(ì‚¬ìš©ìž FQDN) ì„ì¦ - í´ë¼ì–¸íŠ¸ì˜ ë™ì IP ì£¼ì†Œ™€ ì´ë©”ì¼ ì£¼ì†Œë¥¼ í†µí•´ í„°ë„�ì—�ì•¡ì„¸ìŠ¤í• ì ˆì„ ìž¥ì¹˜ë‹¤.

2ë‹¨ê³„. 1ë‹¨ê³„ì—�ì„œ IP Only(*IP ì „ìš©), IP + FQDN(ë„„ë©”ì„ ì´ë¦„) ë˜ëŠ” IP + E-mail Address (User FQDN) Authentication(IP + ì´ë©”ì¼ ì£¼ì†Œ(ì‚¬ìš©ìž FQDN) ì„ì¦)ì„*

ì„ íƒ•œ ê²½ìš° *IP Address(IP ì£¼ì†Œ) í•„ë“œì—* ì›ê²© í´ë¼ì´ì–¸íŠ¸ IP ì£¼ì†Œë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤.

3ë‹¨ê³„. ì•Œê³ ìžˆëŠ” ê²½ìš° ë“œë¡ë‹´ ëª©ë¡ì—ì„œ ì ˆì ˆí•œ ì˜µì…˜ì„ ì„ íƒí•©ë‹ˆë‹¤. IP ì£¼ì†Œë¥¼ ìž…ë ¥í•˜ê±°ë‚˜, 1ë‹¨ê³„ì—ì„œ *IP Only(IP ì „ìš©) ë˜ëŠ” IP + FQDN(Domain Name) Authentication(IP + FQDN) Authentication(IP + E-mail Address(USER FQDN) Authentication)ì„ íƒí•œ* ê²½ìš° DNS ì„œë²„ì—ì„œ IP ì£¼ì†Œë¥¼ í™•ì¸í•©ë‹ˆë‹¤.

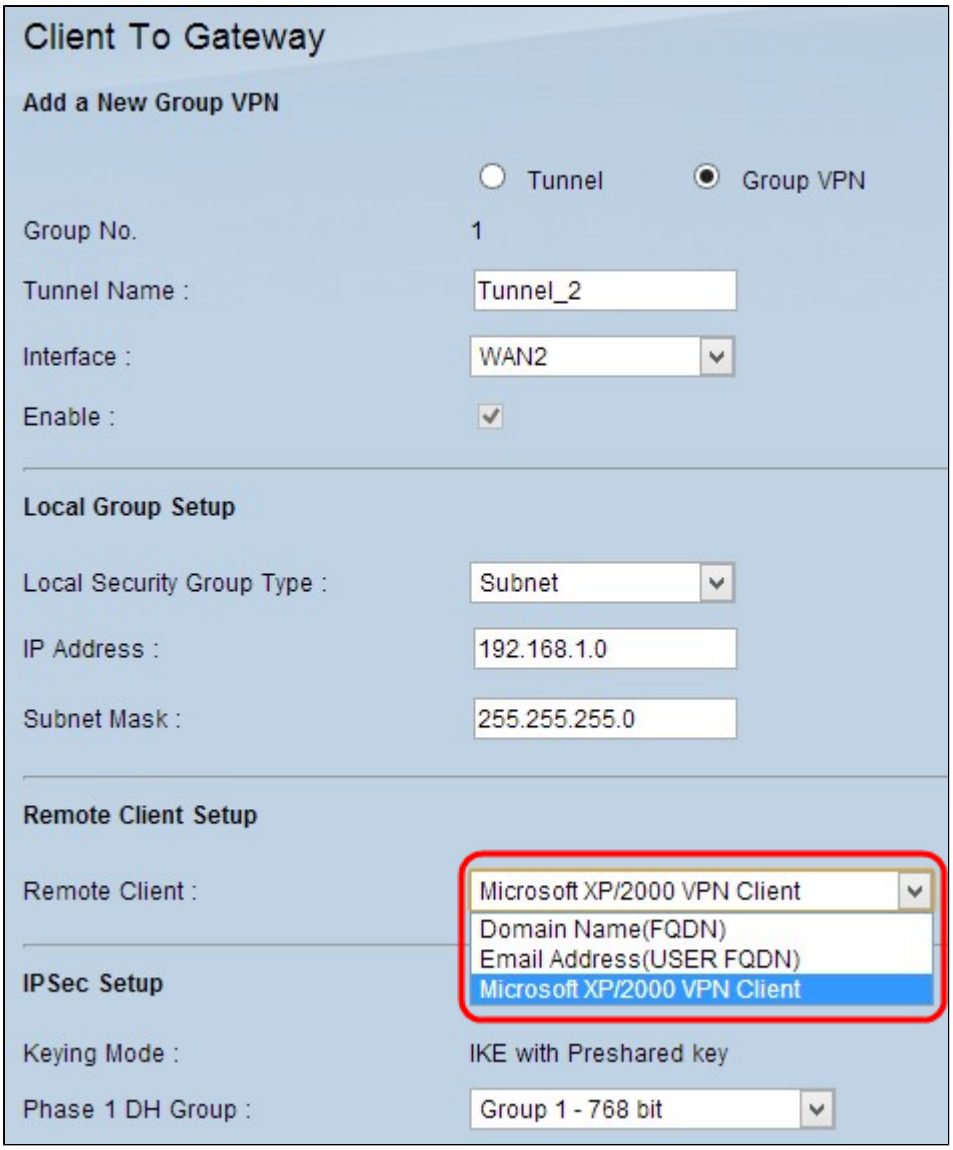
- IP Address - ì›ê²© í´ë¼ì´ì–¸íŠ¸ ê³ ì • IP ì£¼ì†Œë¥¼ ë‚˜íƒ€ë‚´ëŠ” ê³ ì • IP ì£¼ì†Œë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤.
- IP by DNS Resolved - ì›ê²© í´ë¼ì´ì–¸íŠ¸ ê³ ì • IP ì£¼ì†Œë¥¼ ëª¨ë¥´ëŠ” ê²½ìš° DNS ì„œë²„ì¼ë¥¼ íŠµí•´ ìž…ë©™ì œë¡œ IP ì£¼ì†Œë¥¼ ê²€ìƒ‰í•˜ëŠ” IP ì£¼ì†Œë¥¼ ë„£ëŠ” ë©”ì„œ ì´ë¦„ì„ ìž…ë ¥í•©ë‹ˆë‹¤. í•„ë“œì—ì„œ IP ì£¼ì†Œë¥¼ ë„£ëŠ” ìž…ë ¥í•©ë‹ˆë‹¤.

4ë‹¨ê³„. 1ë‹¨ê³„ì—ì„œ IP + FQDN(Domain Name) ì„ íƒ하ëŠ” *ë©™ì • IP + FQDN(Domain Name) ì„ íƒì„ ì„ íƒí•œ* 경우 Domain name í•„ë“œì—ì„œ IP ì£¼ì†Œ *ë„ë©”ì„ ì´ë¦„ì„* ìž…ë ¥í•©ë‹ˆë‹¤.

5ë‹¨ê³„. 1ë‹¨ê³„ì—ì„œ *IP + E-mail Address(USER FQDN) Authentication(IP + E-mail Address(USER FQDN) ì„ íƒ)* ë˜ëŠ” *Dynamic IP + E-mail Address(USER FQDN) Authentication(ë©™ì • IP + E-mail ì£¼ì†Œ(USER FQDN) ì„ íƒ)ì„* ì„ íƒí•œ 경우 Email Address(ì´ë©”ì¼ ì£¼ì†Œ) í•„ë“œì—ì„œ ì´ë©”ì¼ ì£¼ì†Œë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤.

6ë‹¨ê³„. Group(ê·¸ë£¹)ì„ ì„ íƒí•˜ëŠ” Remote Client(ì›ê²© í´ë¼ì´ì–¸íŠ¸) ë“œë¡ë‹´ëª©ì—ì„œ ì ˆì ˆí•œ *Add A New Tunnel(ìƒˆ í„°ë„ ì¶”ê°€)* ì„ ì„ íƒ하ë©´ 1ë‹¨ê³„ì—ì„œ Tunnel VPN(í„°ë„ VPN)ì„ ì„ íƒí•œ 경우 ì´ ë‹¨ê³„ë¥¼ ê±´ë„ˆëœ€ë‹¤.

- FQDN(ë„ë©”ì¸ ì´ë¦„) - ë“±ë¡ëœ ë„ë©”ì¸ ì†µí•´ í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆëŠ” ì ˆì ˆí•œ Domain Name(ë„ë©”ì¸ ì´ë¦„)ì„ ë“±ë¡í•œ ë„ë©”ì¸ ì´ë¦„ì„ ìž…ë ¥í•©ë‹ˆë‹¤.
- ì´ë©”ì¼ ì£¼ì†Œ(ì‚¬ìš©ìžë¥¼ íˆ•ì¸ìž FQDN) - í´ë¼ì´ì–¸íŠ¸ ì´ë©”ì¼ ì£¼ì†Œë¥¼ ì£¼ì†Œë¥¼ í†µí•´ í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆëŠ” ì ˆì ˆí•œ Email Address(ì´ë©”ì¼ ì£¼ì†Œ)ì„ ì„ íƒí•©ë‹ˆë‹¤.
- Microsoft XP/2000 VPN í´ë¼ì´ì–¸íŠ¸ - Microsoft XP ë˜ëŠ” Microsoft 2000 Windows ì†Œí”„íŠ¸ì›¨ì–´ë¥¼ í†µí•´ í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆëŠ” Microsoft VPN í´ë¼ì´ì–¸íŠ¸ 소프트웨어를 사용하는 경우 ì„ íƒí•©ë‹ˆë‹¤. 이 옵션을 사용하는 경우 í„°ë„ì—ì„œ ì•¡ì„¸ìŠ¤í• ìˆ˜ ìžˆëŠ” ì ˆì ˆí•œ 계정을 ì„¤ì •í•´ì•¼ 합니다.



7ë‹¨ê³„. Save(**ì €ìž¥**)ë¥¼ í´ë¦í•˜ì—¬ ì„¤ì •ì„ ì €ìž¥í•©ë‹ˆë‹¤.

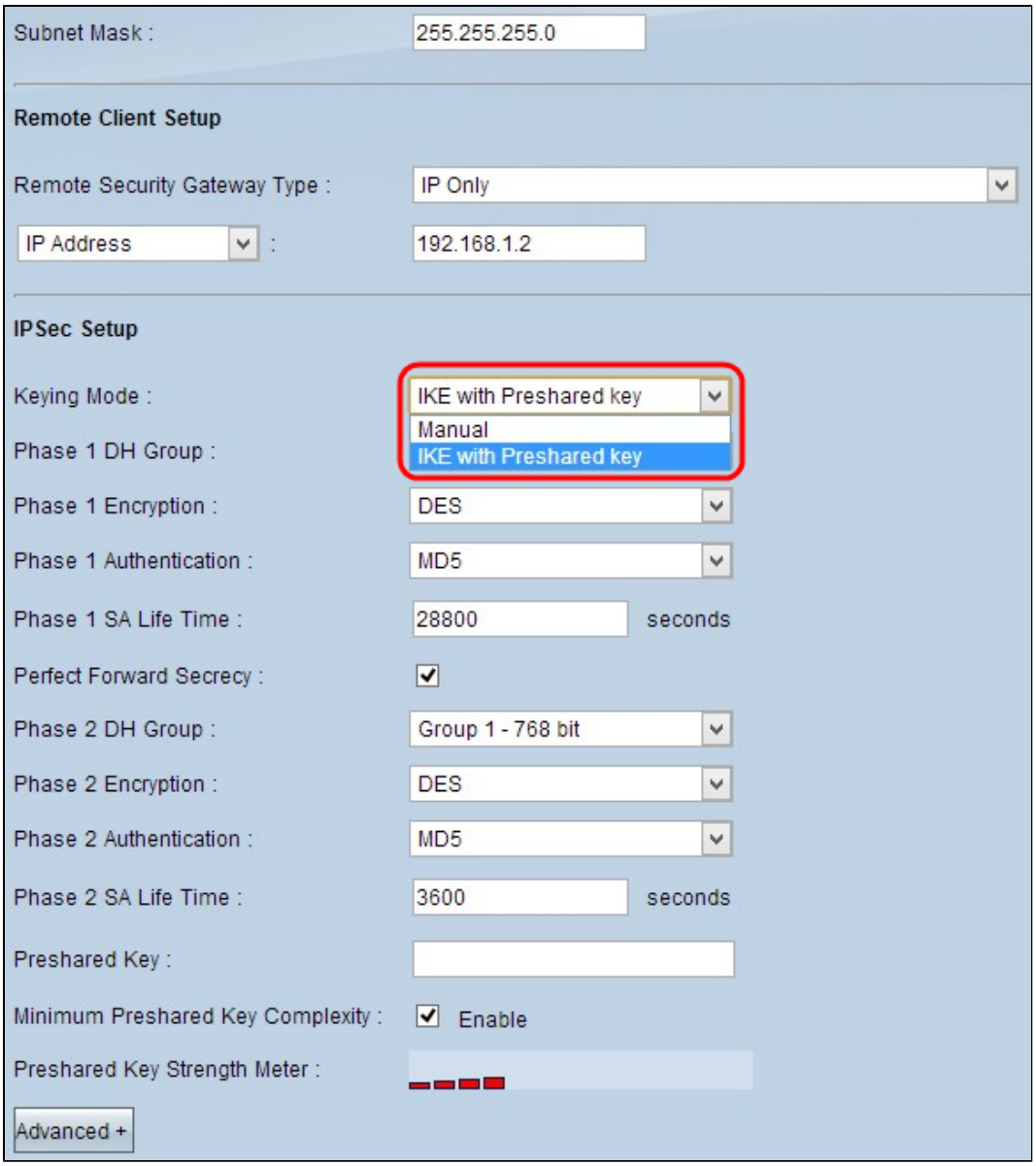
IPSec ì„¤ì •

IPSec(Internet Protocol Security)ì€ íŠ¸ì‹ ì„¸ì…˜ ë°ì´í„°ê·¸ëž¨ ë³´ì•ˆì„ ìœ„í•´ ì—”ë“œ ë³´ì•ˆ ê³¼ì •ì„ ì œê³µí•˜ëŠ” ì œê²©êµí•œ ì§‘í•©ìž…ë‹ˆë‹¤.

ì°¸ê³ : VPNì€ ë‘ ë©´ì—ëŠ” IPSecì´ ìž‘ë™í•˜ê³ ìžˆí™”ë¥¼ ì•ˆì „í•˜ê²Œ ë³´í˜¸í•©ë‹ˆë‹¤. ë˜ëŠ” PFS(Perfect Forward Secrecy) ê¸°ëŠ¥ì„ ì‚¬ìš©ì—¬ ì–‘ì¸¡ì—ì„œ ë™ì¼í•œ í‚¤ë¥¼ ìƒì„±í•©ë‹ˆë‹¤.

1ë‹¨ê³„. Keying Mode ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ ë³´ì•ˆ ì„¤ì •ì— ì‚¬ìš©í• ê´€ë¦¬ *ëª¨ë“œë¥¼ ì„ íƒ*í•©ë‹ˆë‹¤. ê°ë³´ ëª¨ë“œëŠ” ì„¤ì • ê³¼ì •ì˜ ì†ë„ë¥¼ ë†’ì´ì§€ë§Œ ë³´ì•ˆì„ ë‚®ì¶¥ë‹ˆë‹¤. *ì„ íƒí•œ IKEìž…ë‹¤.*

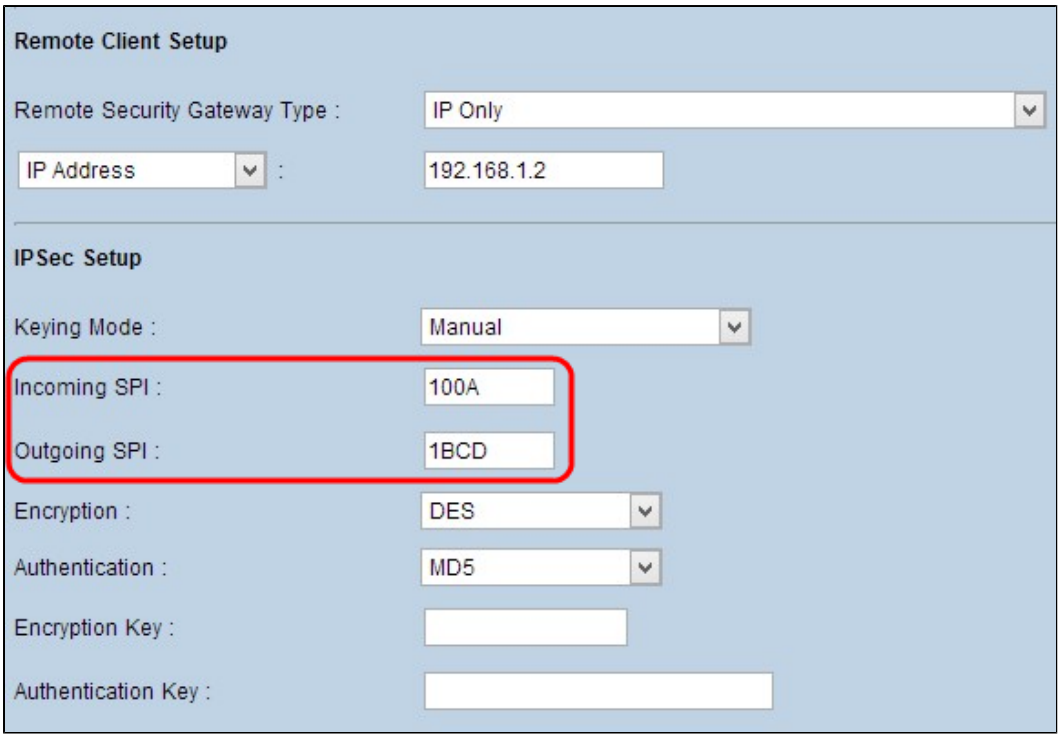
- Manual(ì˜ë™) - ì§€ì ‘ ìƒì„± í‚¤ë¥¼ ìž…ë ¥í•˜ê³ í‚¤ì™€ ì•ŠëŠ” ì‚¬ìš©ìž ì§€ì • ë³´ì•ˆ ëª¨ë“œìž…ë‹ˆë‹¤. ë¬¸ì œ í•´ê²° ë°© ì†Œëª¨ ì • í™˜ê²½ì—ì„œ ì‚¬ìš©í•©ë‹ˆë‹¤. Add A New Tunnel(ìƒˆ í„°ë„ ì¶”ê°€) ì„ ì…˜ì—ì„œ 1ë‹¨ê³„ì—ì„œ Group VPN(ê·¸ë£¹ VPN)ì„ ì„ íƒí•œ ê²½ìš° ì´ ì˜µì…˜ë§Œ ë¨¼ì €ì•¼ í•©ë‹ˆë‹¤.
- ì‚¬ìš© ê°€ëŠ¥í•œ IKE - IKE(Internet Key Exchange) í”„ë¡œí† ì½œì€ í„°ë„ì—ì„œ ëŒ€í•œ ì¸ì¦ ì„¤ì •ì„ ê°„ì†Œí™”í•©ë‹ˆë‹¤ ê°€ëŠ¥í•œ ë°©ë²•ì„ ì‚¬ìš©í•©ë‹ˆë‹¤.



ì˜ë�™ í‚¤ ëª¨ë“œ ì»¨í”¼ê·¸ ˆì�ˆ…˜

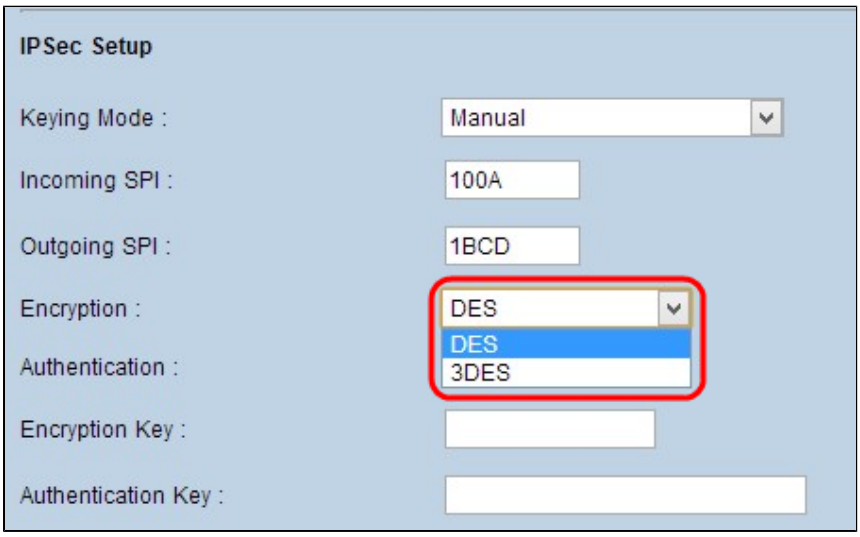
1ë‹¨ê³„. Incoming SPI(Security Parameter Index) í•„ë“œì—� SPIì—� ëŒ€í•œ ê³ ìœ 16ì§„ì˜ *ê°’ì�„* ìž…ë ¥í•©ë‹ˆë‹¤. SPIëŠ” ì˜¨ì‹ íŒ¨í‚·ì—� ëŒ€í•œ ë³´í˜¸ë¥¼ í•¨ê» ê²°ì •í•©ë‹ˆë‹¤. ESP(Encapsulating Security Payload Protocol) í—¤ë�”ì—�ì„œ ì „ë‹¬ë�©ë‹ˆë‹¤. 100ë¶€í„° ffffffffê¹Œì§€ ìž…ë ¥í• ì˜ˆìƒ‰ë‹ˆë‹¤. ë¡œì»¬ ë�¼ìš°í„°ì�˜ ì˜¨ì‹ SPIëŠ” ì›�ê²© ë�¼ìš°í„°ì�˜ ë°œì‹ SPIì™€ ì�¼ì¹˜í•´ì•¼ í•©ë‹ˆë‹¤.

2ë‹¨ê³„. Outgoing SPI(Security Parameter Index) í•„ë“œì—� SPIì�˜ ê³ ìœ 16ì§„ì˜ *ê°’ì�„* ìž…ë ¥í•©ë‹ˆë‹¤. SPIëŠ” ë°œì‹ íŒ¨í‚·ì—� ëŒ€í•œ ë³´í˜¸ë¥¼ í•¨ê» ê²°ì •í•©ë‹ˆë‹¤. ESP(Encapsulating Security Payload Protocol) í—¤ë�”ì—�ì„œ ì „ë‹¬ë�©ë‹ˆë‹¤. 100ë¶€í„° ffffffffê¹Œì§€ ìž…ë ¥í•´ì˜¨ ìž‰ì‰µë‹ˆë‹¤. ì›�ê²© ë�¼ìš°í„°ì�˜ ë‚˜ê°€ëŠ” SPIëŠ” ë¡œì»¬ ë�¼ìš°í„°ì�˜ ë“¤ì–´ì˜¤ëŠ” SPIì™€ ì�¼ì¹˜í•´ì•¼ í•©ë‹ˆë‹¤.



3ë‹¨ê³„. Encryption ë“œë¡ë‹¤ìš´ ëª©ë¡�ì—�ì„œ ë�°ì�´í„°ì—� ì •í•©í•œ ì•”í˜¸í™” ë°©ë²•ì�„ ì„ íƒ•í•©ë‹¤. ê¶Œìž¥ë�˜ëŠ” ì•”í˜¸í™”ëŠ” *3DESìž…ë‹¤*. VPN í„°ë„�ì�€ ì–‘ìª½ ë��ì—� ë�™ì¼•œ ì•”í˜¸í™” ë°©ë²•ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹¤.

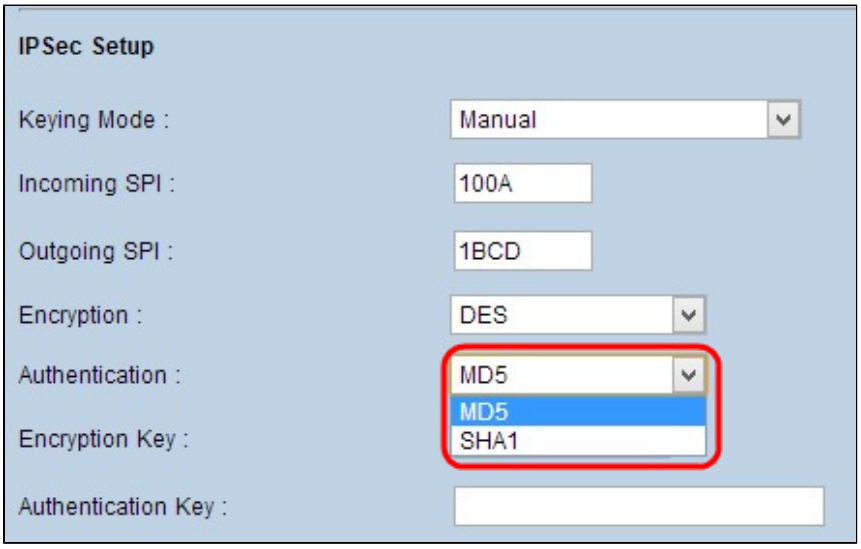
- DES - DES(Data Encryption Standard)ëŠ” ë�°ì�´í„° ì•”í˜¸í™”ì—� 56ë¹„íŠ¸ í‚¤ë¥¼ ì‚¬ìš©í•©ë‹¤. DESëŠ” ì˜¤ëž˜ë�˜ì—ˆìœ¼ë°˜ í•˜ë‚˜ì�˜ ì—”ë“œí�¬ì¸íŠ¸ê°€ DESë§Œ ì§€ì›�í•˜ëŠ” ê²½ìš°ì—�ë§Œ ì‚¬ìš©í•´ì•¼ í•©ë‹¤.
- 3DES - 3DES(Triple Data Encryption Standard)ëŠ” 168ë¹„íŠ¸ì�˜ ê°„ë‹¨í•œ ë°©ë²•ìž…ë‹¤. 3DESëŠ” ë�°ì�´í„°ë¥¼ ì„¸ ë²ˆ ì•”í˜¸í™”í•˜ë¯€ë¡œ DESë³´ë‹¤ ë�” ê°•ë ¥í•œ ë³´ì•ˆì�„ ì œê³µí•©ë‹¤.



4ë‹¨ê³„. *Authentication* ë“œë¡ë‹¤ìš´ ëª©ë¡�ì—�ì„œ ë�°ì�´í„°ì—� ì •í•©í•œ ì•”ì¸ì¦ ë°©ë²•ì�„ ì„ íƒ•í•©ë‹¤. MD5ë³´ë‹¤ ì•ˆ „í•˜ê³¤ ê¶Œìž¥ë�˜ëŠ” ì•ˆì¦ì¦ë²• SHA*1*ìž…ë‹¤. VPN í„°ë„�ì�€ ì–‘ìª½ ë��ì—� ë�™ì¼•œ ì•ˆì¦ì¦ ë°©ë²•ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹¤.

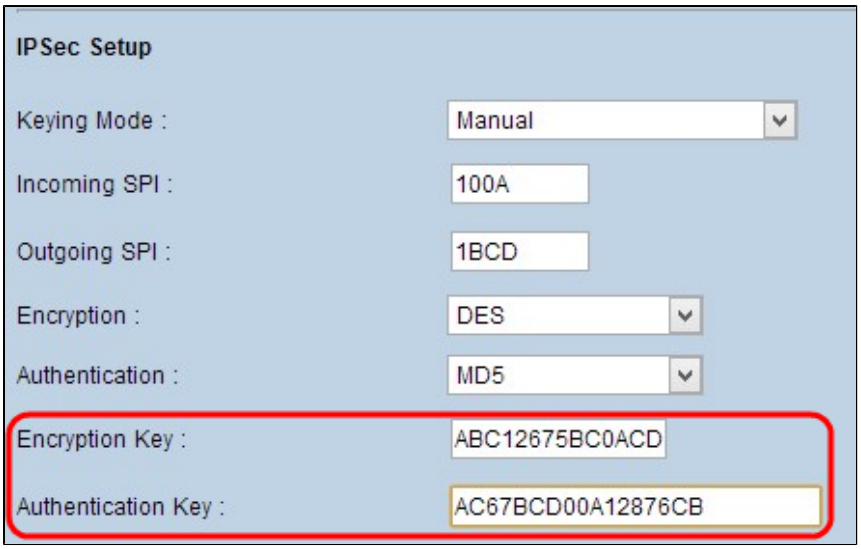
- MD5 - MD5(Message Digest Algorithm-5)ëŠ” ì²´ê¬ì„¬ ê³„ì‚°ì¼œë¡œ ì•...ì�˜ ì•ˆ

ê³µê²©ìœ¼ë¡œë¶€í„° ë�°ì�´í„°ë¥¼ ë³´í˜¸í•˜ëŠ” 32ìž�ë¦¬ 16ì§„ìˆ˜ í•´ì‹œ í•¨ìˆ˜ë¥¼ ë‚˜íƒ€ëƒ…ë‹ˆë‹¤.
- SHA1 - SHA1(Secure Hash Algorithm version 1)ì�€ 160ë¹„íŠ¸ í•´ì‹œ í•¨ìˆ˜ë¡œ MD5ë³´ë‹¤ ì•ˆ ì „í•˜ì§€ë§Œ ê³„ì‚°í•˜ëŠ” ë�° ì‹œê°„ì�´ ë�” ê±¸ë¦½ë‹ˆë‹¤.



5ë‹¨ê³„. Encryption Key(ì•”í˜¸í™” í‚¤) í•„ë“œì—� ë�°ì�´í„°ë¥¼ ì•”í˜¸í™”í•˜ê³ í•´ë�…í• í‚¤ë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤. 3ë‹¨ê³„ì—�ì„œ ì•”í˜¸í™” ë°©ë²•ìœ¼ë¡œ DESë¥¼ ì„ íƒ�í•˜ëŠ” ê²½ìš° 16ìž�ë¦¬ 16ì§„ìˆ˜ ê°’ì„ ìž…ë ¥í•©ë‹ˆë‹¤. 3ë‹¨ê³„ì—�ì„œ ì•”í˜¸í™” ë°©ë²•ìœ¼ë¡œ 3DESë¥¼ ì„ íƒ�í•œ ê²½ìš° 40ìž�ë¦¬ 16ì§„ìˆ˜ ê°’ì„ ìž…ë ¥í•©ë‹ˆë‹¤.

6ë‹¨ê³„. Authentication Key(ì¸ì¦ í‚¤) í•„ë“œì—� ìŠ¤ëž˜ì‹œì„ ì¸ì¦ì•Œê³ ë¦¬ì¦˜ í‚¤ë¥¼ ìž…ë ¥í•©ë‹ˆë‹¤. 4ë‹¨ê³„ì—�ì„œ MD5ë¥¼ ì¸ì¦ ë°©ë²•ìœ¼ë¡œ ì„ íƒ�í•˜ëŠ” ê²½ìš° 32ìž�ë¦¬ 16ì§„ìˆ˜ ê°’ì„ ìž…ë ¥í•©ë‹ˆë‹¤. 4ë‹¨ê³„ì—�ì„œ ì¸ì¦ ë°©ë²•ìœ¼ë¡œ SHAë¥¼ ì„ íƒ�í•˜ëŠ” ê²½ìš° 40ìž�ë¦¬ 16ì§„ìˆ˜ ê°’ì„ ìž…ë ¥í•©ë‹ˆë‹¤. VPN í„°ë„ì€ ì–‘ë½ ë��ì—� ë™ì¼í•œ ì¸ì¦ ê³µìœ í‚¤ë¥¼ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.



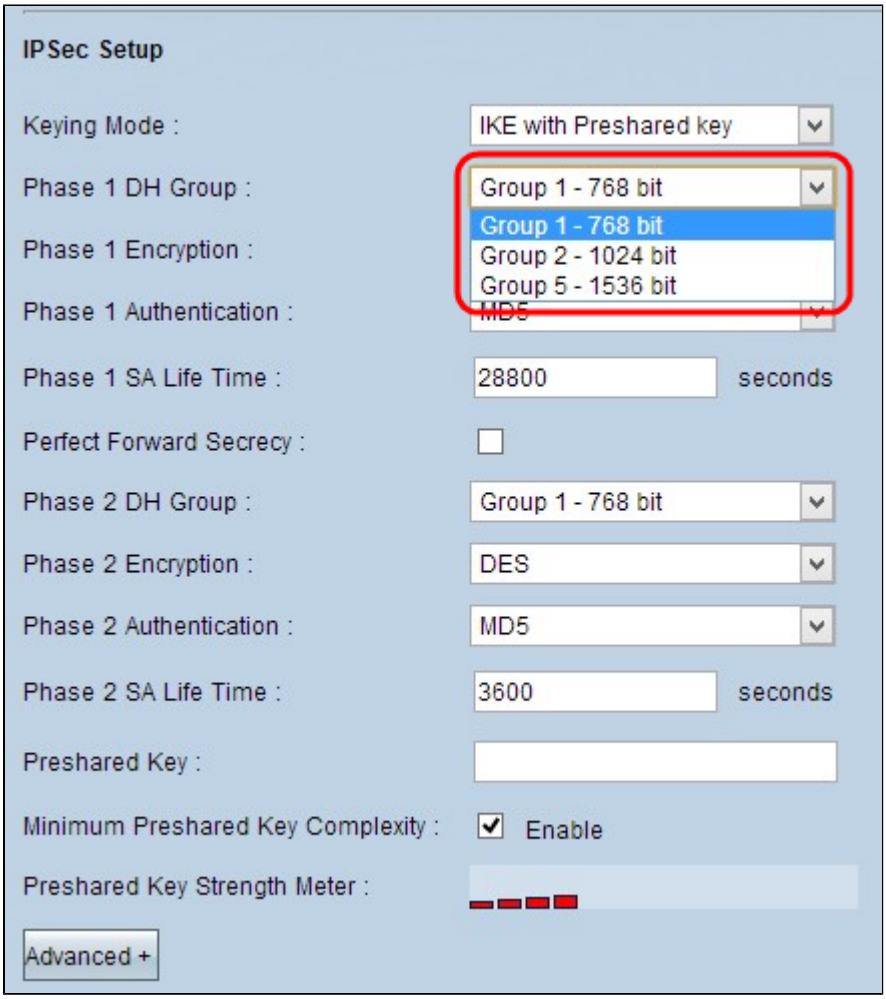
7ë‹¨ê³„. Save(ì €ìž¥)ë¥¼ í´ë¦í•˜ì—¬ ì„¤ì •ì„ ì €ìž¥í•©ë‹ˆë‹¤.

ì„¤ì • ê³µìœ í‚¤ ë³€ê²½ì»¨í”¼ê·¸ë ˆì´ì…˜ IKE

1ë‹¨ê³„. Phase 1 DH Group ë“œë¡ë‹¤ìš´ ëª©ë¡ì—�ì„œ ì ˆí•œ *Phase 1 DH* Groupì„

ì„ íƒ•í•©ë‹ˆë‹¤. 1ë‹¨ê³„ëŠ” ì•ˆì „í•œ ì—°ì¦ ì§€ì›í•˜ê°ˆ ìœ„í•´ ë•Œ ê°„ì— í•œ SA(Logical Security Association)ë¥¼ ì„¤ì •í•©ë‹ˆë‹¤. DH(Diffie-Hellman)ëŠ” 1ë‹¨ê³„ ì¤‘ì— í‚¤ì—°ì¦ ì•Œê³ ë¦¬ì¦˜ì„ ì•ˆì „í•˜ê²Œ í•©ë‹ˆë‹¤. ê·¸ë£¹ ì‹ë³„ìžëŠ” ì—°ì¦ ì—°ì‚° ë¹„ë°€ í‚¤ì˜ ê¸¸ì´ë¥¼ ê²°ì •í•©ë‹ˆë‹¤.

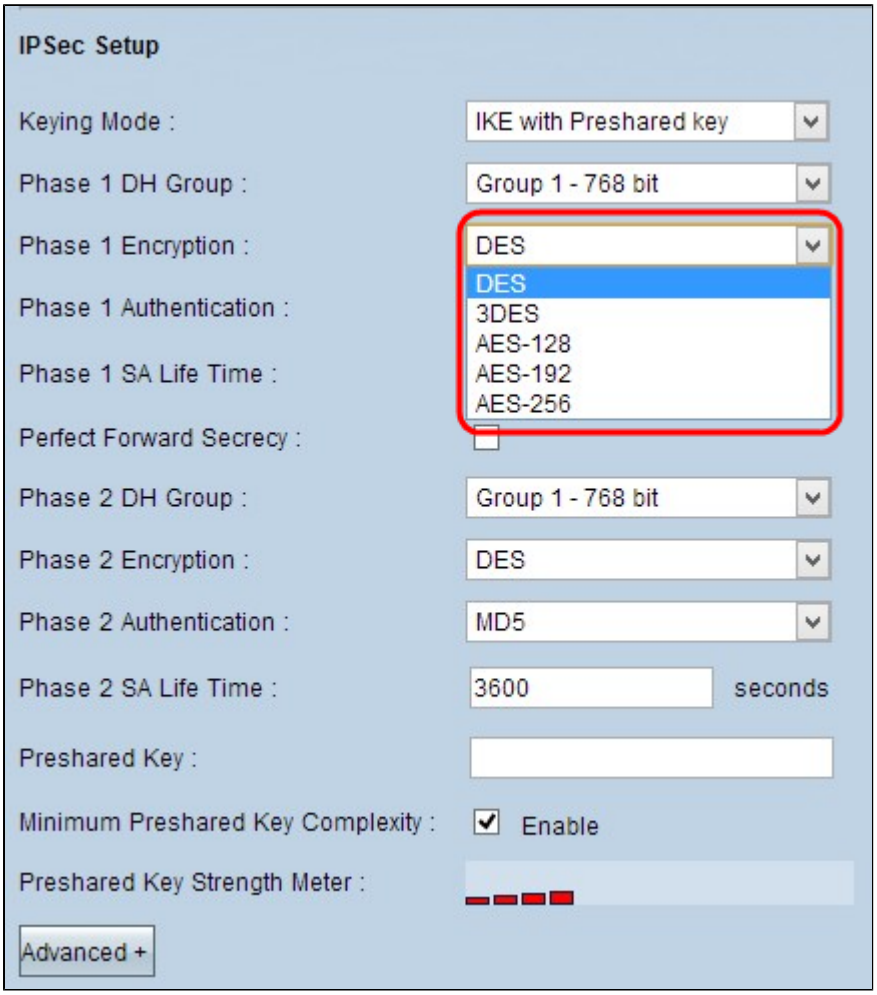
- ê·¸ë£¹ 1 - 768ë¹„íŠ¸ - ê°€ìž¥ ë‚®ì€ ì´ˆê¸° í‚¤ ê°€ìž¥ ì•ˆ „í•˜ì§€ ì•Šì€ ì—°ì¦ ê·¸ë£¹ìž…ë‹ˆë‹¤. ê·¸ë£¹ 1ì€ ë„ë¦¬ ì§€ì›ë˜ì§€ë§Œ ì†ë„ê°€ ë‚®ì€ ë„¤íŠ¸ì›Œí¬ì—¬ì•¼ í•©ë‹ˆë‹¤.
- ê·¸ë£¹ 2 - 1024ë¹„íŠ¸ - ë" ë†'ì€ ì´ˆê¸° í‚¤ì™€ ë" ì•ˆ „í•œ ì—°ì¦ ê·¸ë£¹ìž…ë‹ˆë‹¤. ê·¸ë£¹ 1ë¡œ IKE í‚¤ë¥¼ ê³„ì‚°í•˜ëŠ ë°°ëŠ ì‹œê°„ì´ ë„ˆë¬´ ì˜¤ëž˜ ê±¸ë¦´ ê²½ìš° ì‚¬ìš©í•©ë‹ˆë‹¤.
- Group 5 - 1536ë¹„íŠ¸ - ê°€ìž¥ ê°•ë ¥í•œ í‚¤ì™€ ê°€ìž¥ ì•ˆ „í•œ ì—°ì¦ ê·¸ë£¹ìž…ë„ ë‚˜íƒ€ë‚˜ë…ˆë‹¤. IKE í‚¤ë¥¼ ê³„ì‚°í•˜ëŠ ë°° ì‹œê°„ì´ ë" í•„ìš"í•©ë‹ˆë‹¤. ë„íŠ¸ì›Œí¬ ì†ë„ê°€ ë¹ ë¥¸ ê²ƒì´ ì¢‹ìŠµë‹ˆë‹¤.



2ë‹¨ê³„. Phase 1 Encryption(1ë‹¨ê³„ ì•"í˜¸í™") ë"œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ í‚¤ë¥¼ ì•"í˜¸í™"í•˜ëŠ ë°° ì ˆí•œ 1ë‹¨ê³„ ì•"í˜¸í™"ë¥¼ ì„ íƒ•í•©ë‹ˆë‹¤. ê°€ìž¥ ì•ˆ „í•œ ì•"í˜¸í™" ë°©ë²•ì€ë¡œ 3DESë¥¼ ì‚¬ìš©í•˜ëŠ" ê²ƒì´ ì¢‹ìŠµë‹ˆë‹¤. VPN í„°ë„ì€ ì–'ìª½ ë••ì— ë™ì¼í•œ ì•"í˜¸í™" ë°©ë²•ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.

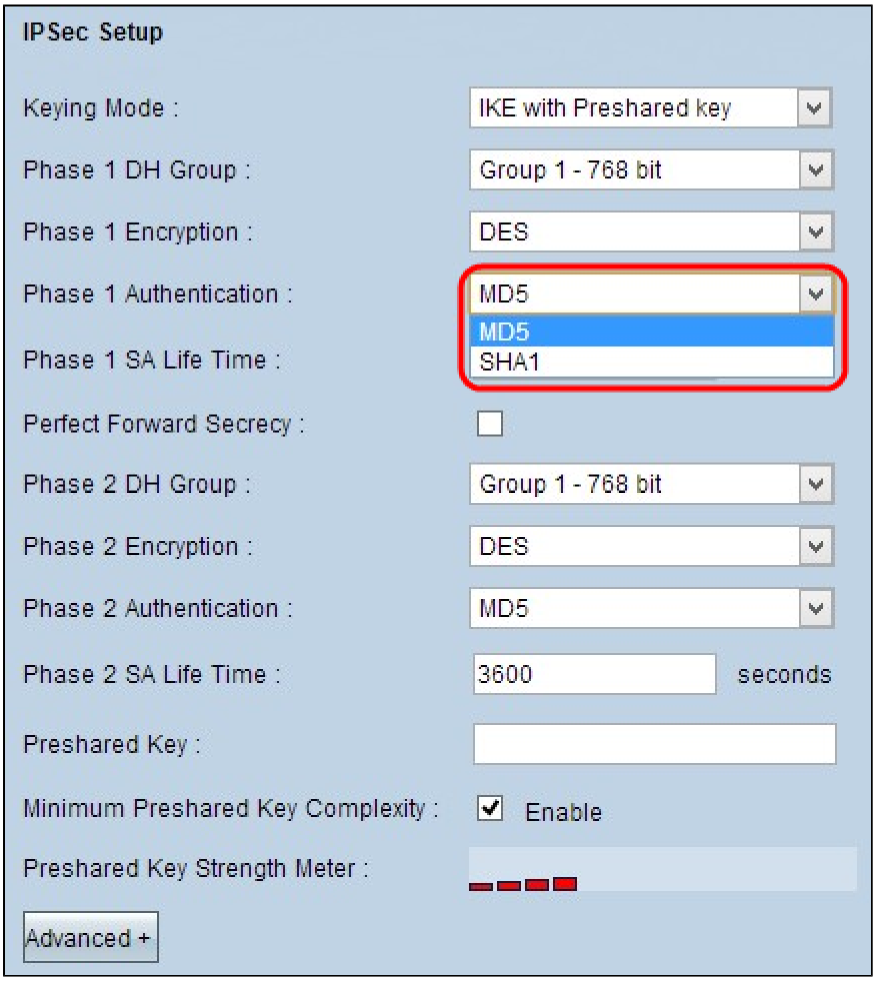
- DES - DES(Data Encryption Standard)ëŠ" ë°°ì€ í‚¤ 길ì´ë¡œ 56ë¹„íŠ¸ í‚¤ í¬ê¸°ë¥¼ ì‚¬ìš©í•©ë‹ˆë‹¤. DESëŠ" ì˜¤ëž˜ë˜ì—ˆì¼ë©° í•˜ë‚˜ì˜ ì—"ë"œí¬ì¸íŠ¸ê°€ DESë§Œ ì§€ì›í•˜ëŠ" ê²½ìš°ì—ë§Œ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.
- 3DES - 3DES(Triple Data Encryption Standard)ëŠ" 168ë¹„íŠ¸ì˜ ê°„ë‹¨í•œ ì•"í˜¸í™" ë°©ë²•ìž…ë‹ˆë‹¤. 3DESëŠ" ë°°ì´ì „ë¥¼ ë²ˆ ì•"í˜¸í™"í•˜ëŠ ë¡œ DESë³´ë‹¤ ë" ê°•í•¨ í•œ ë³´ì•ˆì„ ì œê³µí•©ë‹ˆë‹¤.
- AES-128 - AES(Advanced Encryption Standard)ëŠ" 128ë¹„íŠ¸ ì•"í˜¸í™" ë°©ë²•ìœ¼ë¡œ ì„ë°˜

í…ìŠ¤íŠ¸ë¥¼ 10íšŒì˜ ë°˜ë³µ ê³¼ì •ì„ ì•”í˜¸í™”í•©ë‹ˆë‹¤.
- AES-192 - AES(Advanced Encryption Standard)ëŠ” ì¼ë°˜ í…ìŠ¤íŠ¸ë¥¼ 12íšŒì˜ ë°˜ë³µì„ í†µí•´ ì•”í˜¸í™”í•©ë‹ˆë‹¤. AES-192ëŠ” AES-128ë³´ë‹¤ ì•ˆ „í•©ë‹ˆë‹¤.
- AES-256 - AES(Advanced Encryption Standard)ëŠ” 256ë¹„íŠ¸ ì•”í˜¸í™” ë°©ë²•ìœ¼ë¡œ ì¼ë°˜ í…ìŠ¤íŠ¸ë¥¼ 14íšŒì˜ ë°˜ë³µ ê³¼ì •ì„ ì•”í˜¸í™”í•©ë‹ˆë‹¤. AES-256ì€ ê°€ìž¥ ì•ˆ „í•œ ì•”í˜¸í™” ë°©ë²•ìž…ë‹ˆë‹¤.



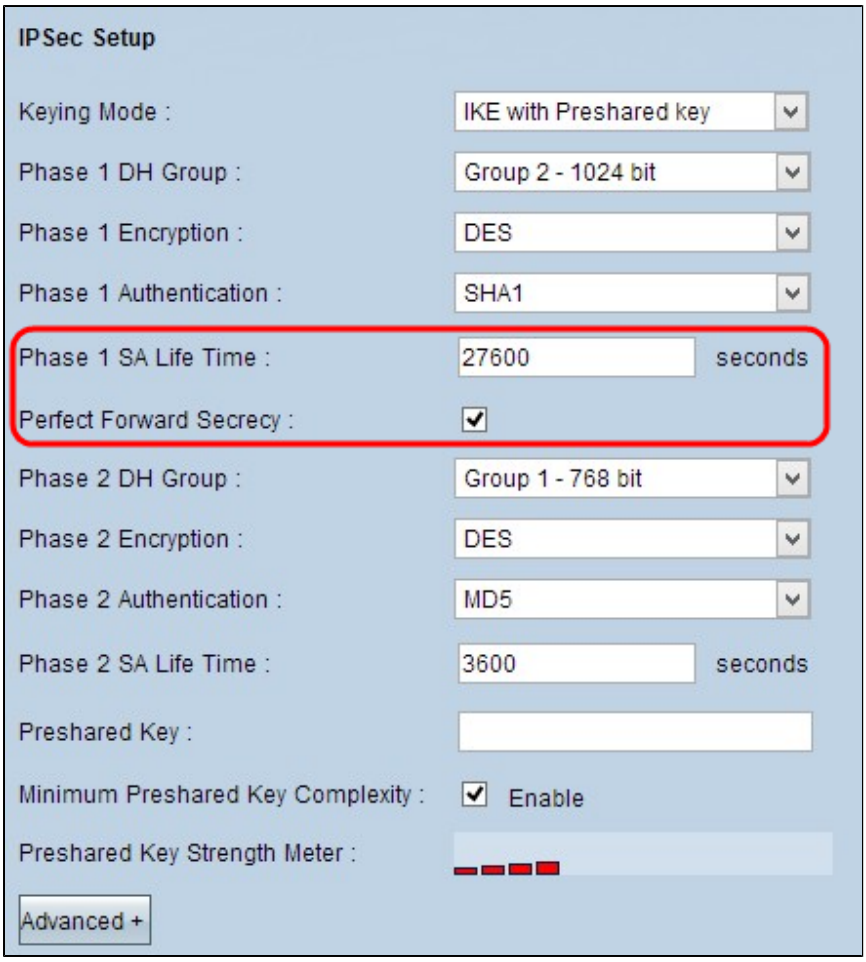
3ë‹¨ê³„. Phase 1 Authentication ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ ì› ê²© *Phase 1* ì¸ì¦ ë°©ë²•ì„ ì„ íƒí•©ë‹ˆë‹¤. VPN í„°ë„ì€ ì–‘ìª½ ë••ì— ë™™ì¼í•œ ì¸ì¦ ë°©ë²•ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.

- MD5 - MD5(Message Digest Algorithm-5)ëŠ” ì²´í¬ì„¬ ê³„ì‚°ì„ì•…ìš© ì•…ì„± ê³µê²©ìžê°€ ë°°ì´í„°ë¥¼ ë³€ê²½í•˜ëŠ” 32ìž�ë¦¬ 16ì§„ìˆ˜ í•´ì‹œ ê°’ìž…ë¥¼ ë‚˜íƒ€ë‚´ëŠ” ë°ì´í„° ë¬´ê²°ì„± ì•Œê³ ë¦¬ì¦˜ìž…ë‹ˆë‹¤.
- SHA1 - SHA1(Secure Hash Algorithm version 1)ì€ 160ë¹„íŠ¸ í•´ì‹œ í¨ìˆ˜ë¡œ MD5ë³´ë‹¤ ì•ˆ „í•˜ì§€ë§Œ ê³„ì‚°í•˜ëŠ” ë° ì‹œê°„ì´ ë” ê±¸ë¦½ë‹ˆë‹¤.



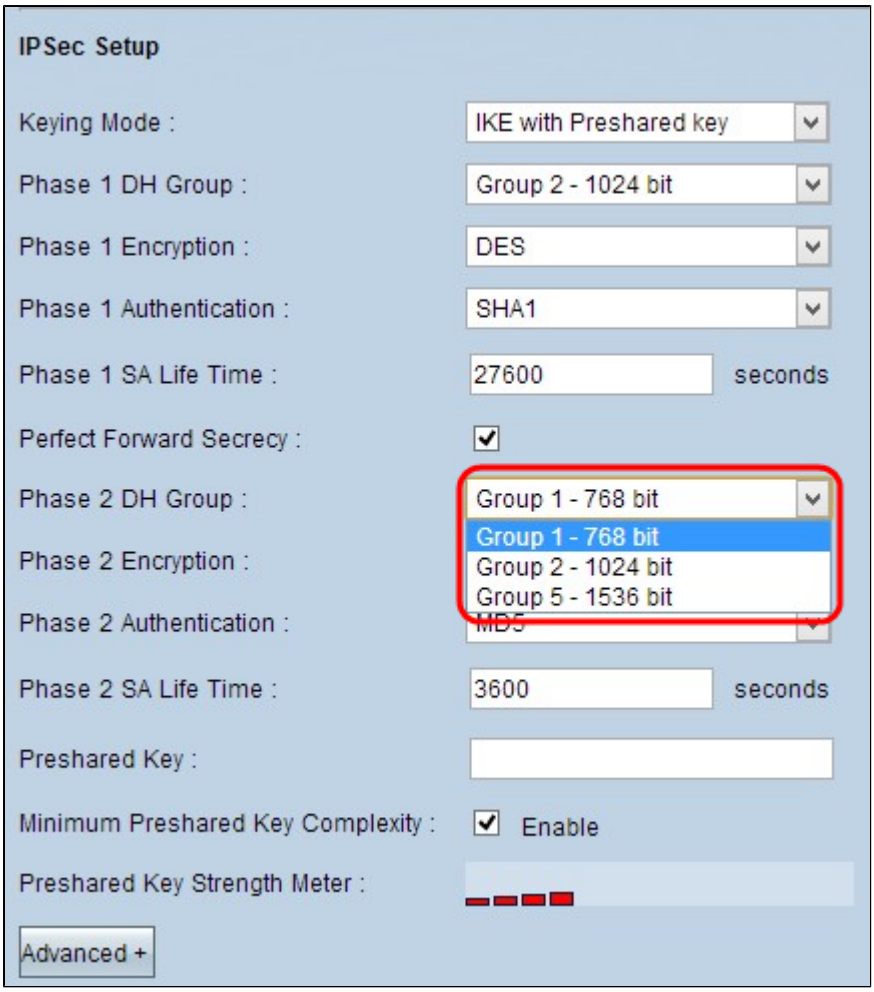
4ë‹¨ê³„. 1ë‹¨ê³„ í‚¤ê°€ ìœ íš¨í•˜ê³ VPN í„°ë„ì´ í™œì„± ìƒíƒœë¡œ ìœ ì§€ë˜ëŠ” ì‹œê°„ì„ 1ë‹¨ê³„ SA ìˆ˜ëª… í•„ë“œì— ì´ˆ ë‹¨ìœ„ë¡œ ìž…ë ¥í•©ë‹ˆë‹¤.

5ë‹¨ê³„. í‚¤ì— ëŒ€í•œ ë³´í˜¸ë¥¼ ìœ„í•´ Perfect Forward Secrecy í™•ì¸ëž€ì„ ì„ íƒí•©ë‹ˆë‹¤. ì´ ì˜µì…˜ì„ ì‚¬ìš©í•˜ë©´ í‚¤ê°€ ì†ìƒë˜ë”ë¼ë„ ê²½ìš° ë°ì´í„°ë¥¼ ë³´í˜¸í•˜ê¸° ìœ„í•´ ìƒˆ í‚¤ë¥¼ ìƒì„±í• ìˆ˜ ìžˆìŠµë‹ˆë‹¤. ì•”í˜¸í™”ë¥¼ ë°ì´í„°ë¥¼ ê°€ì§€ë¡œ í‚¤ë¥¼ í†µí•´ì„œ ê°€ì§€ë„ë¡ ëŒ€ëž¼ ì„œ í‚¤ê°€ ìƒì„±ë˜ë”ë¼ë„ ë‹¤ë¥¸ í‚¤ë¥¼ ë³´í˜¸í•˜ê¸° ë•Œë¬¸ì— ì´ì „ í‚¤ ì •ë³´ì— ì˜í•´ ì•ˆì „í•˜ì§€ ì•Šì„ ìˆ˜ ìžˆìŠµë‹ˆë‹¤. ì´ëŠ” ë³´ì•ˆì´ ê°•í™”ë˜ë¯€ë¡œ ê¶Œìž¥ë˜ëŠ” ì˜µì…˜ìž…ë‹ˆë‹¤.



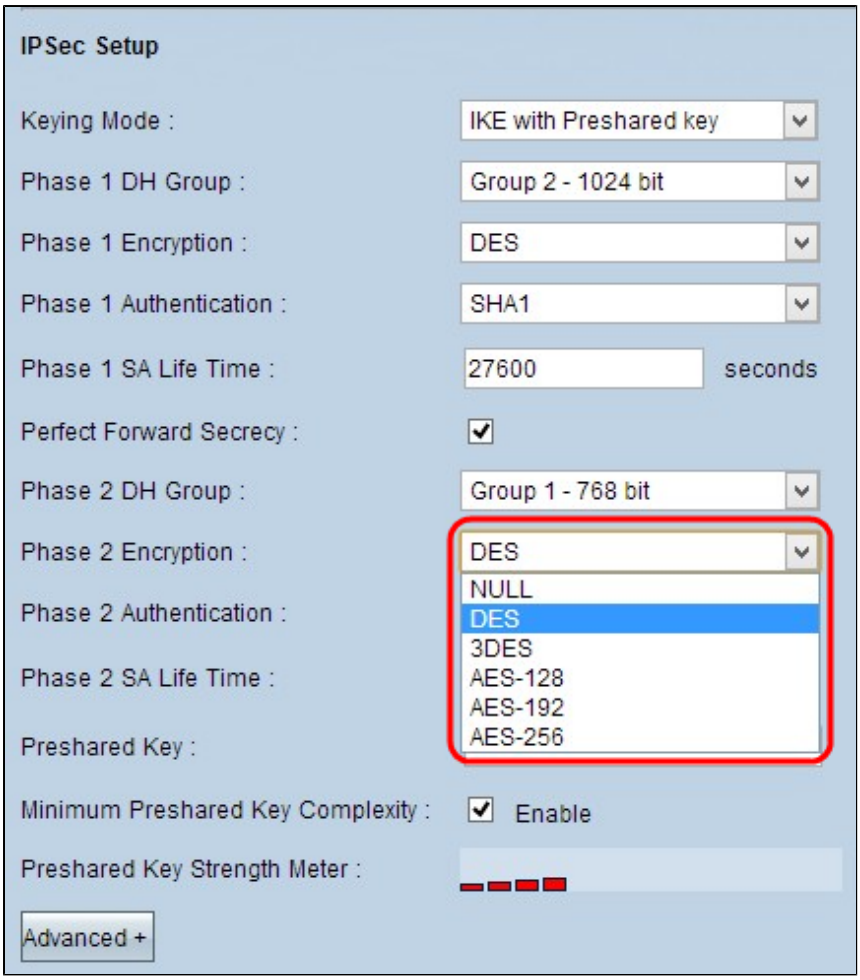
6ë‹¨ê³„. Phase 2 DH Group ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ ì ˆ ì ˆí•œ *Phase 2 DH* Groupì„ ì„ íƒí•©ë‹ˆë‹¤. 2ë‹¨ê³„ì—ì„œ ë³´ì•ˆ ë³´ì´ì•ˆ ì—°ê²°ì„ ì„¤ì •í•˜ê¸° ìœ„í•´ ë™ì¼í•œ ì„¤ì •ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.

- Group 1 - 768 bit(ê·¸ë£¹ 1 - 768ë¹„íŠ¸) - ê°€ìž¥ ë‚®ì€ 1 - 768ë¹„íŠ¸ í‚¤ì™€ ê°€ìž¥ ì•ˆ „í•˜ì§€ ì•Šì€ ì¸ì¦ ê·¸ë£¹ì„ ë‚˜íƒ€ëƒ…ë‹ˆë‹¤. ê·¸ëŸ¬ë‚˜ IKE í‚¤ë¥¼ ê³„ì‚°í•˜ëŠ” ë°° ì‹œê°„ì´ ë” ê²Œ ê±¸ë¦½ë‹ˆë‹¤. ë„¤íŠ¸ì›Œí¬ ì†ë„ê°€ ë‚®ì€ ê²½ìš° ì†Œí”„íŠ¸ì›¨ì–´ ë„¤íŠ¸ì›Œí¬ ì†ë„ê°€ ë‚®ì€ ê²½ìš°.
- Group 2 - 1024ë¹„íŠ¸ - ë” ê°•ë ¥í•œ í‚¤ì™€ ë” ì•ˆ „í•œ ì¸ì¦ ê·¸ë£¹ì„ ë‚˜íƒ€ëƒ…ë‹ˆë‹¤. ê·¸ëŸ¬ë‚˜ IKE í‚¤ë¥¼ ê³„ì‚°í•˜ëŠ” ë°° ì‹œê°„ì´ ë” ê±¸ë¦½ë‹ˆë‹¤.
- Group 5 - 1536ë¹„íŠ¸ - ê°€ìž¥ ê°•ë ¥í•œ í‚¤ì™€ ê°€ìž¥ ì•ˆ „í•œ ì¸ì¦ ê·¸ë£¹ì„ ë‚˜íƒ€ëƒ…ë‹ˆë‹¤. IKE í‚¤ë¥¼ ê³„ì‚°í•˜ëŠ” ë°° ì‹œê°„ì´ ë” ê±¸ë¦½ë‹ˆë‹¤. ë„¤íŠ¸ì›Œí¬ ì†ë„ê°€ ë¹ ë¥¸ ê²ƒì´ ì¢‹ìŠµë‹ˆë‹¤.



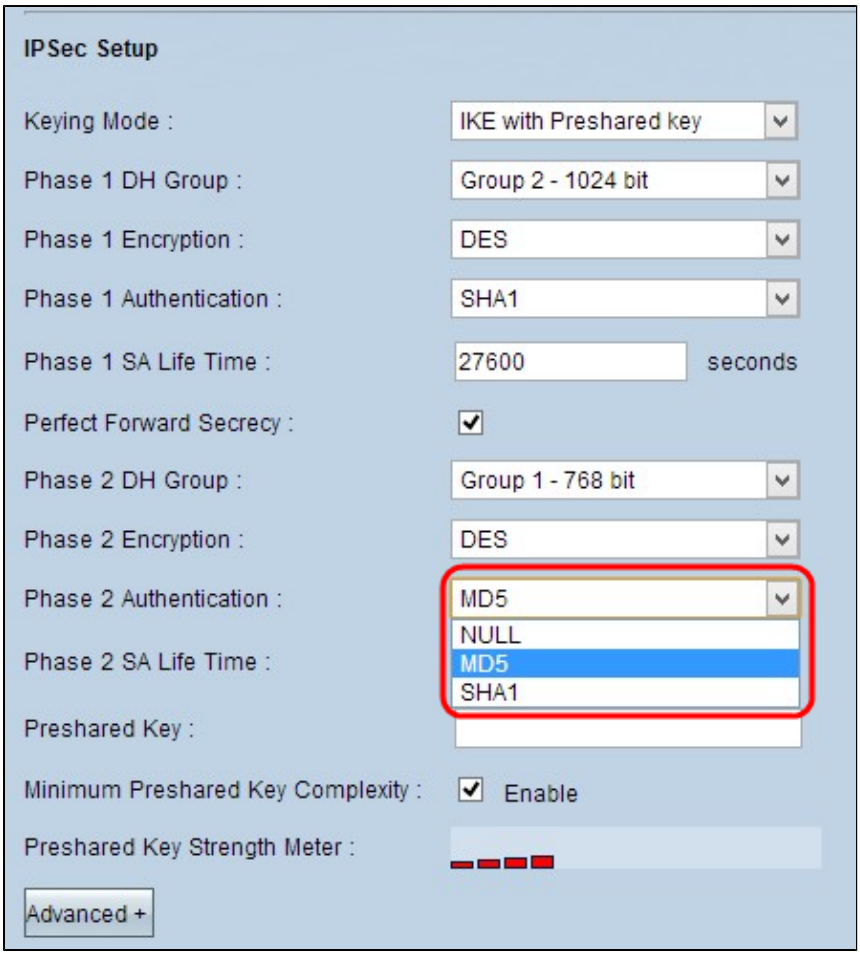
7ë‹¨ê³„. Phase 2 Encryption ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì—¬ì„¯ í‚¤ì›Œë“œ ì•”í˜¸í™” ë°©ì‹ì„ *Phase 2 Encryption*ì€ ì„ íƒ•í•©ë‹ˆë‹¤. ê°€ìž¥ ì•ˆì „í•œ ì•”í˜¸í™” ë°©ë²•ì€ AES-256ì´ê³ ê¶Œìž¥ë©©ë‹ˆë‹¤. VPN í„°ë„ì€ ì–‘ìª½ ë••ì— ë©™ì¼•œ ì•”í˜¸í™” ë°©ë²•ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.

- DES - DES(Data Encryption Standard)ëŠ” ë°°ì´„° ì•”í˜¸í™”ì— 56ë¹„íŠ¸ í‚¤ í©¬ê¸°ë¥¼ ì‚¬ìš©í•©ë‹ˆë‹¤. DESëŠ” ì˜¤ëž˜ë©ˆì—ˆìœ¼ë©° í•˜ì© ì—”ë“œíŠ¸ê°€ DESë§Œ ì§€ì›©í•˜ëŠ” ê²½ìš°ì—©ë§Œ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.
- 3DES - 3DES(Triple Data Encryption Standard)ëŠ” 168ë¹„íŠ¸ì©˜ ê°„ë‹¨í•œ ì•”í˜¸í™” ë°©ë²•ìž…ë‹ˆë‹¤. 3DESëŠ” ë°°ì´„°ë¥¼ ì„¸ ë²ˆ ì•”í˜¸í™”í•˜ë©€ DESë³´ë‹¤ ë•” ê°•í•œ ë³´ì•ˆì œ ì œê³µí•©ë‹ˆë‹¤.
- AES-128 - AES(Advanced Encryption Standard)ëŠ” 128ë¹„íŠ¸ ì•”í˜¸í™”ë¡œ ì©¼ë°˜ í……ìŠ¤íŠ¸ë¥¼ 10íšŒì©˜ ë°˜ë³µ ê³¼ì • •ì„œ ê±°ì³ ì•”í˜¸í™”í•©ë¡œ ë³€í™˜í•©ë‹ˆë‹¤.
- AES-192 - AES(Advanced Encryption Standard)ëŠ” ì©¼ë°˜ í……ìŠ¤íŠ¸ë¥¼ 12íšŒì©˜ ë°˜ë³µì©„ í†µí•´ ì•”í˜¸í™”í•©ë¡œ ë³€í™˜í•˜ëŠ” 192ë¹„íŠ¸ ì•”í˜¸í™”ìž…ë‹¤. AES-192ëŠ” AES-128ë³´ë‹¤ ì•ˆ „í•©ë‹ˆë‹¤.
- AES-256 - AES(Advanced Encryption Standard)ëŠ” 256ë¹„íŠ¸ ì•”í˜¸í™”ë¡œ ì©¼ë°˜ í……ìŠ¤íŠ¸ë¥¼ 14íšŒì©˜ ë°˜ë³µ ê³¼ì • •ì„œ ê±°ì³ ì•”í˜¸í™”í•©ë¡œ ë³€í™˜í•©ë‹ˆë‹¤. AES-256ì€ ê°€ìž¥ ì•ˆì „í•œ ì•”í˜¸í™”ìž…ë‹¤.



8ë‹¨ê³„. Phase *2* Authentication ë“œë¡ë‹¤ìš´ ëª©ë¡ì—ì„œ ì ˆí•œ ì•”í˜¸í™” ë°©ë²•ì„ ì„ íƒí•©ë‹ˆë‹¤. VPN í„°ë„ì€ ì–‘ìª½ ë••ì— ë™ì¼í•œ ì•”í˜¸í™” ë°©ë²•ì„ ì‚¬ìš©í•´ì•¼ í•©ë‹ˆë‹¤.

- MD5 - MD5(Message Digest Algorithm-5)ëŠ” ì²´í¬ì„¬ ê³„ì‚°ì œë¡œ ì•…ì©Œ ê³µê²©ìœ¼ë¡œë¶€í„° 32ìž©ë¦¬ 16ì§„ìˆ˜ í•´ì‹œ í•¨ìˆ˜ë¥¼ ë‚˜íƒ€ëƒ…ë‹ˆë‹¤.
- SHA1 - SHA1(Secure Hash Algorithm version 1)ì€ 160ë¹„íŠ¸ í•´ì‹œ í•¨ìˆ˜ë¡œ MD5ë³´ë‹¤ ì•ˆì „í•œ ê³„ì‚°ì´ ëŠë¦¬ë¯€ë¡œ ë³´ì•ˆì´ ê°•í™”ëœ ê³„ì‚°ì„ ì‚¬ìš©í•©ë‹ˆë‹¤.
- Null - ì¸ì¦ ë°©ë²•ì´ ì‚¬ìš©ë˜ì§€ ì•ŠìŠµë‹ˆë‹¤.



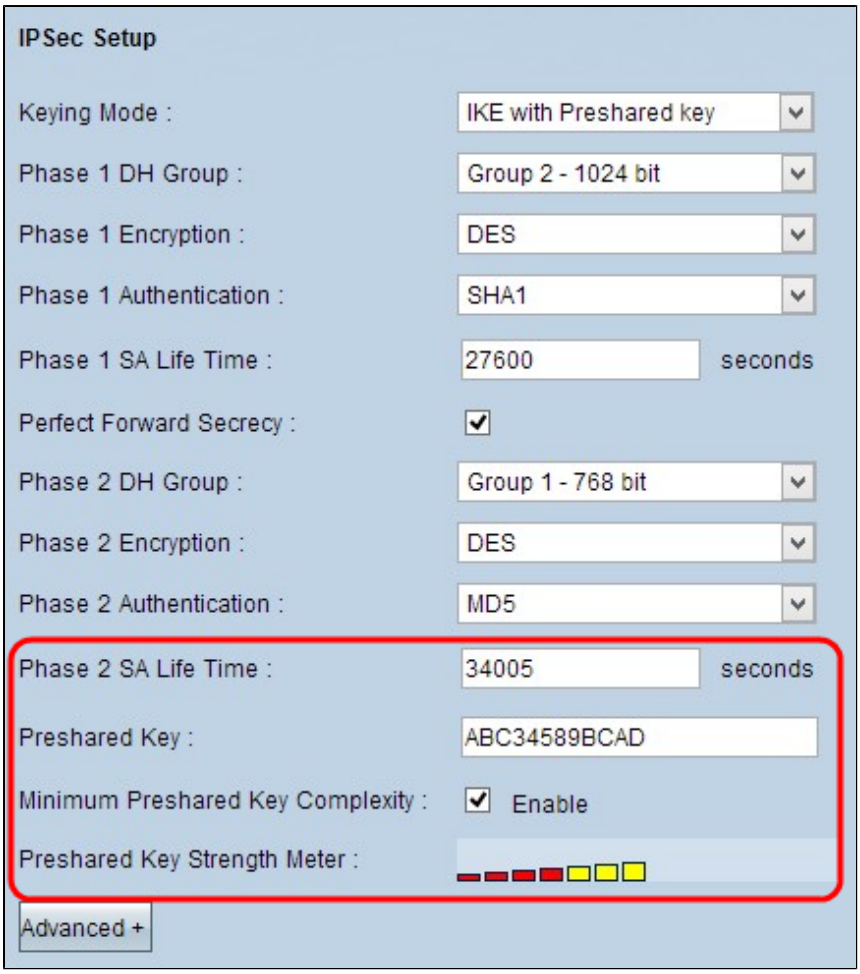
9ë‹¨ê³„. Phase 2 í‚¤ê°€ ìœ íš¨í•˜ê³ VPN í„°ë„ì› ì´ í™œì„±í™”ëì œ ìœ ì§€ë˜ìž ìœ¼ë©´ ì‹œê°„ì„ Phase 2 *SA Life Time í•„ë“œì—* ìž…ë ¥í•©ë‹¤.

10ë‹¨ê³„. Preshared Key(ì‚¬ì „ ê³µìœ í‚¤) í•„ë“œì— í”¼ì–´ë¥¼ ì›ì¹ ¦ í•˜ê°€ ìœ„í•´ IKE í”¼ì–´ ê°„ì— ì›ê³ ê³µìœ ë˜ëŠ” ë¹„ë°€ í‚¤ë¥¼ ìž…ë ¥í•©ë‹¤. ìµœëŒ€ 30ê°œì›Ž 16ì§„ìˆ˜ ë° ë¬¸ìž›ë¥¼ ì‚¬ìš© í•œëŠ ìˆ˜ ìžˆìŠµë‹¤. VPN í„°ë„ì›€ì–´ì²½ ë››ì— ë›™ì›íœ ì‚¬ìš© í•œëŠ ì‚¬ìš©í•´ì•¼ í•©ë‹¤.

ì°¸ê³ : VPNì›´ ì•ˆ „í•˜ê²Œ ìœ ì§€ë˜ë„ë¡ IKE í”¼ì–´ ê°„ì›˜ ì‚¬ìš© í•œëŠ ìž›ì£¼ ë³€ê²½í•˜ëŠ ê²ƒì´ ì¢‹ìŠµë‹¤.

11ë‹¨ê³„. ì‚¬ì „ ê³µìœ **í‚¤ìž—** ëŒ€íœ ê°•ë„ ì¸ì •ê¸°ë¥¼ í™œì„±í™”í•˜ë ¤ë©´ Minimum Preshared Key Complexity í™•ì›ëž€ì„ ì„ íƒí•©ë‹¤. ìƒˆë‘ ë§‰ëŒ€ê°€ ì†µí•´ ì‚¬ìš© í‚¤ì˜ ê°•ë„ë¥¼ ë¶„ì„í•©ë‹¤.

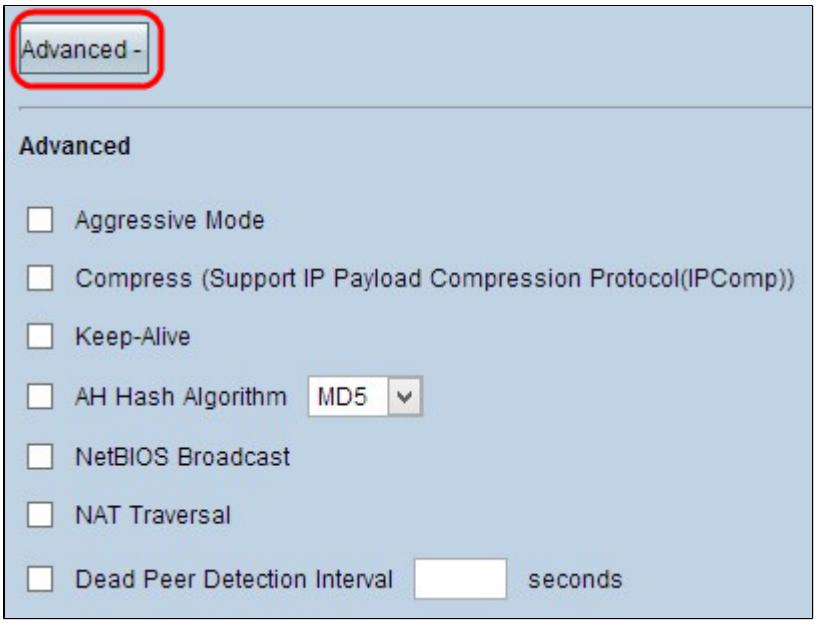
ì°¸ê³ : *ì‚¬ìš© í‚¤ì¸ ê°•ë„ì¸ì •ê¸°ë¥¼ ë§‰ëŒ€ê°€ ì†µí•´ ì‚¬ìš© í‚¤ì˜ ê°•ë„ë¥¼ í™•ì›ì›œ ì‚¬ìš© ê°•ëŠ¥ê°€ ë…¸ìž¥ê³¼ ë…¸ìž¥ì—ê²Œ ì—°ê²°ëœ ë‚´ë¶€ ë„¤íŠ¸ì›Œí¬ì— ì—°ê²°ëœ ë‚´ë¶€ ë„¤íŠ¸ì›Œí¬ë¥¼ ë³´í˜¸í•©ë‹¤.*



12ë‹¨ê³„. Save(ì €ìž¥)ë¥¼ í´ë¦í•˜ì—¬ ì„¤ì •ì„ ì €ìž¥í•©ë‹ˆë‹¤.

ì‚¬ìš© ê³µë¨ë“œ ì»¨íŽ¸ì§‘ êµ¬ì„± IKE

1ë‹¨ê³„. Advanced(ê³ ê‰)ë¥¼ í´ë¦í•˜ì—¬ Preshared í‚¤ê°€ ìžˆëŠ” IKEì •ì˜ ê³ ê‰ ì„¤ì •ì„ í‘œì‹œí•©ë‹ˆë‹¤.

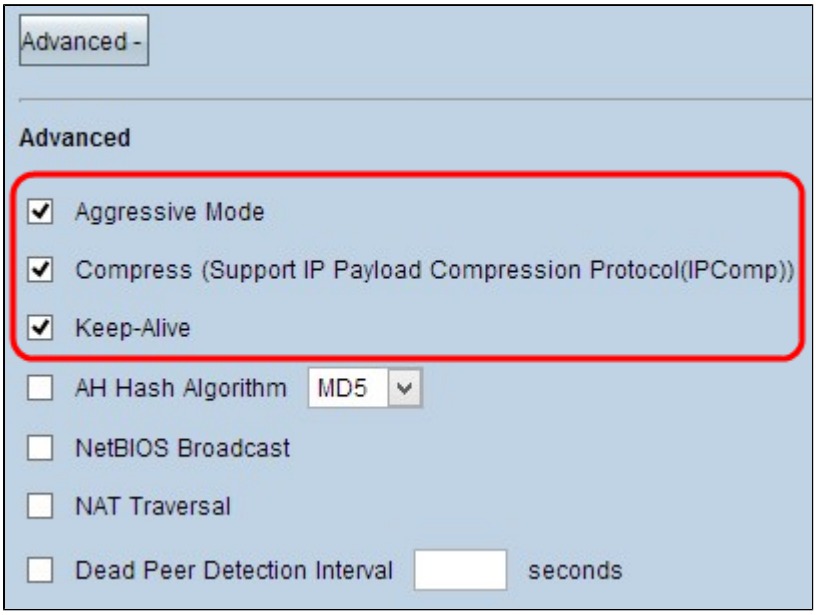


2ë‹¨ê³„. ë„¤íŠ¸ì›Œí¬ ì†ë„ê°€ ë‚®ì€ ê²½ìš° Aggressive Mode í™•ì„±ëž€ì„ ì„ íƒí•©ë‹ˆë‹¤. ì´ë ‡ê²Œ í•˜ë©´ SA ì—°ê²°(1ë‹¨ê³„) ì¤‘ì— ì „ë„ì†¡ IDê°€ ì¼ë¶€ í…ìŠ¤íŠ¸ë¡œ êµ¬íšë˜ê¸° ë•Œë¬¸ì— ì‹œìŠ¤í…œì´ ì‹§ì§€ë§Œ ë³´ì•ˆì€ ë–¨ì–´ì§‘ë‹ˆë‹¤.

ì°¸ê³ : ê·¸ëž¼ì´ì–íŠ¸ì™€ ê²Œì´íŠ¸ì›¨ì´ VPN ì—°ê²°ì—ì„œ Aggressive Modeë¥¼ ì‚¬ìš©í• ìˆ˜ ì—†ìŠµë‹ˆë‹¤.

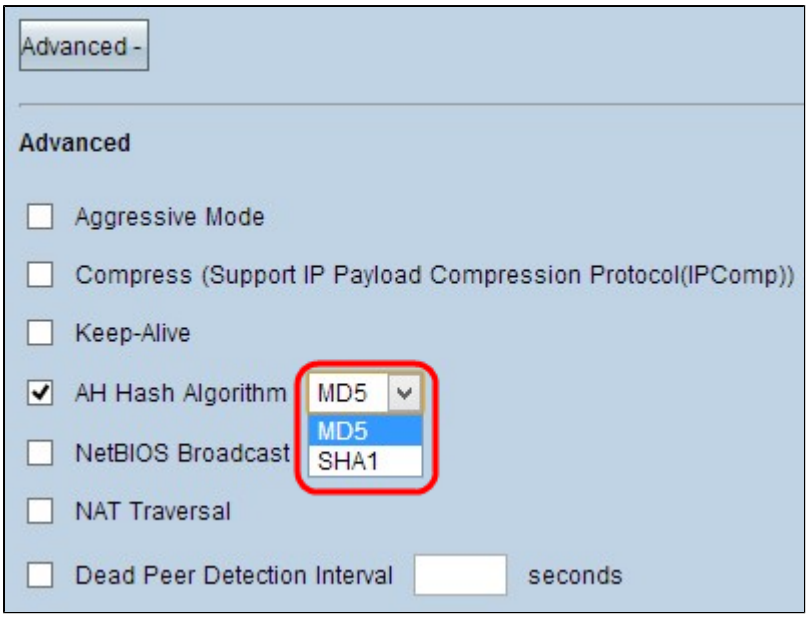
3ë‹¨ê³„. IP ë°°ì´ í„°ê·¸ëž˜ì¨ **í¬ê¸°ë¥¼ ì••ì¶•í•˜ë ¤ë©´ Compress (Support IP Payload Compression Protocol (IPComp))(ì••ì¶•(IPComp(IP íŽ˜ì´ë¡œë“œ ì••ì¶• í”„ë¡œí† ì½œ ì§€ì›))))** í™•ì¸ëž€ì„ ì„ íƒí•©ë‹ˆë‹¤. IPCompëŠ” IP ë°°ì´ í„°ê·¸ëž˜ì¨ í¬ê¸°ë¥¼ ì••ì¶•í•˜ëŠ” ë°° ì‚¬ìš©ë˜ëŠ” IP ì••ì¶• í”„ë¡œí† ì½œìž…ë‹ˆë‹¤. IP ì••ì¶•ì€ ë„¤íŠ¸ì›Œí¬ì†¡ ì†ë„ê°€ ëŠ˜ë¦¬ê³ ì„œë²„ì—ì„œ ì²˜ë¦¬í•˜ëŠ” ë°ì´í„°ì˜ ì–‘ì„ ì¤„ìž…ë‹ˆë‹¤.

4ë‹¨ê³„. í•¨ê» VPN **í„°ë„ì—˜ ì—°ê²°**ì„ í™œì„±í™”í•˜ë ¤ë©´ ì‚¬ìš©ìž ì§€ê·¸ë¦¬ê³ Keep-Alive í™•ì¸ëž€ì„ ì„ íƒí•©ë‹ˆë‹¤. Keep Aliveë¥¼ ì‚¬ìš©í•˜ë©´ ë¹„í™œì„±ëž ê²½ìš° ì¦‰ì‹œ ì—°ê²°ì„ ë‹¤ì‹œ ì•• ì˜ ìž¬ì„¤ì •ë©ë‹ˆë‹¤.



5ë‹¨ê³„. AH(**Authenticate Header**)ë¥¼ í™œì„±í™”í•˜ë ¤ë©´ AH Hash Algorithm í™•ì„±ëž€ì„ ì„ íƒí•©ë‹ˆë‹¤. AHëŠ” ì›ëž¸ ë°°ì´ í„°ì— ëŒ€í•œ ì¸ì¦, ì²´í¬ì„¬ì„ ì¶”ê°€í•˜ì—¬ ë¬´ê²°ì„± ë° IP í—¤ë”ì„± ë³´ì¥ì„ ì œê³µí•©ë‹ˆë‹¤. í„°ë„ì€ ì–´ì²½ì— ëŒ€í•´ ì•…ì„±ì— ë™ìž¦ì„ ì‚¬ìš©í•©ë‹ˆë‹¤.

- MD5 - MD5(Message Digest Algorithm-5)ëŠ” ì²´í¬ì„¬ì„ ì•…ìš©ì œë¡œ ì•…ì˜ ê³µê²©ìžê°€ 128ìž¬ë¦¬ 16ì§„ì˜ í•´ì‹œ í•¨ìˆ˜ë¥¼ ë‚˜íƒ€ë‚´ëŠ” ë°ì´í„°ë¥¼ ë³€ê²½í•˜ì§€ ëª»í•˜ë„ë¡ í•©ë‹ˆë‹¤.
- SHA1 - SHA1(Secure Hash Algorithm version 1)ì€ 160ë¹„íŠ¸ í•´ì‹œ í•¨ìˆ˜ë¡œ MD5ë³´ë‹¤ ì•ˆ „í•˜ì§€ë§Œ ê³„ì‚°ì´ ëŠë¦¬ê³ ë©” ì‹œì§€ ë‹¤ì´ì œ스트를 ìƒì„±í•©ë‹ˆë‹¤.

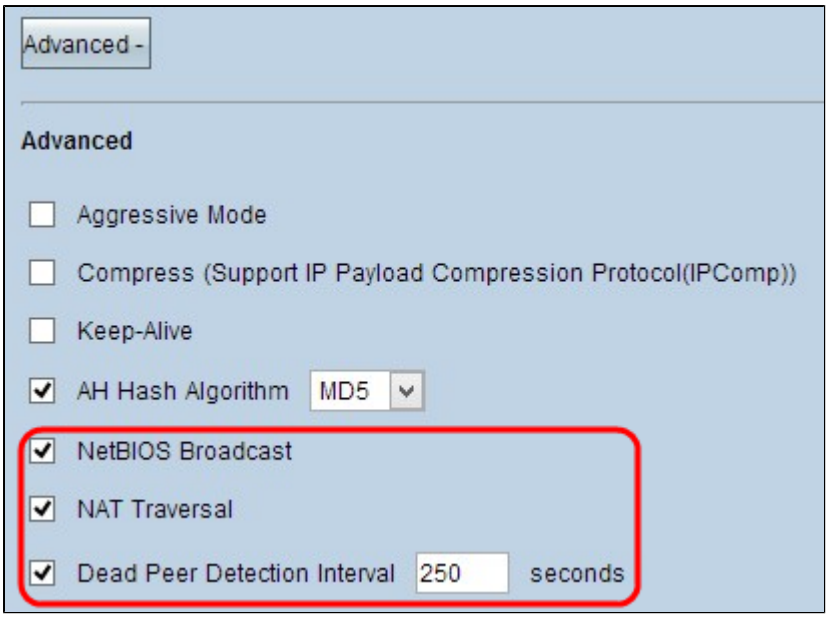


6ë‹¨ê³„. VPN **í„°ë„ì„ ** í†µí•œ ë¼ìš°íŒ… ë¶ˆê°€ íŠ¸ëž˜í”½ì„ í—ˆìš©í•˜ë ¤ë©´ NetBIOS Broadcastë¥¼ ì„ íƒí•©ë‹ˆë‹¤. ê·¸ë³´ê°€ì„ ì„ íƒ ì·¨ì†Œí•˜ë‹¤ë‹¤. NetBIOSëŠ” Network Neighborhoodì™€ ê°™ì€ ì¼ë¶€ ì• í”Œë¦¬ì¼€ì´ì…˜ ë°° Windows ê¸°ëŠ¥ì„ í†µí•´ ë„¤íŠ¸ì›Œí—¬ì—ì„œ íŒŒì¼ê³¼ ì»´í“¨í„°, ì»´í“¨ë“±ê³¼ ê°™ì€ ë¦¬ì†Œë¥¼ ê³µìœ í•˜ëŠ” ë° ì‚¬ìš©ë©©ë‹ˆë‹¤.

7ë‹¨ê³„. ê³µìš© IP **ì£¼ì†Œë¥¼** í†µí•´ ì‚¬ìš© LANì—ì„œ ì›¹ í¬ë·´ì—ì„œ ì•¡ì„¸ìŠ¤í•˜ë ¤ë©´ NAT Traversal í™•ì›ëž€ì›„ ì„ íƒí•©ë‹ˆë‹¤. VPN ë¼ìš°í„°ê° NAT ê²Œì´íŠ¸ì›¨ì´ ë’¤ì—ì„œ ìžˆëŠ” ê²½ìš° NAT í†µê³¼ë¥¼ í™œì„±í™”í•˜ë ¤ë©´ ì›´ í•©ì›¨ì´ ì„ íƒí•©ë‹ˆë‹¤. í„°ë„ì›˜ ì–‘ìª½ ë••ì—ì„œ ë™ì¼í•œ ì„¤ì • ì›´ ìž¬ì–‘í•©ë‹ˆë‹¤.

8ë‹¨ê³„. Dead **Peer Detection Interval(ë•°ë“œ í”¼ì–´ íƒì§€** ê°„ê²©)ì›„ ì„ íƒí•©ë‹ˆë‹¤. ì£¼ê¸°ì ìœ¼ë¡œ hello ë˜ëŠ” ACKë¥¼ í†µí•´ VPN í„°ë„ì›˜ í™œì„±í™”í•©ë‹ˆë‹¤. ì›´ í™•ì›ëž€ì›„ ì„ íƒí•œ ê²½ìš° ì›íí•˜ëŠ” hello ë©”ì‹œì§€ì›˜ ê¸°ê°„ ë˜ëŠ” ê²©ì›„ ìž…ë ¥í•©ë‹ˆë‹¤.

ì°¸ê³ : ê· ë£¹ í›ë••ì›´ì–´íŠ¸ê²Œì›´íŠ¸ì›¨ì›´ VPN ì—°ê²°ì›´ ì•„ë‹Œ ë‹¤ì›¨ í›ë••ì›´ì–´íŠ¸ê²Œì›´íŠ¸ì›¨ì›´ VPN ì—°ê²°ì—›ì›„ ëŒ€í•´ì„œëŠ Dead Peer Detection Intervalì›„ êµ¬ì„±í• ìˆ˜ ìžˆìµë‹ˆë‹¤.



9ë‹¨ê³„. Save(**ì €ìž¥**)ë¥¼ í´ë¦í•˜ì—¬ ì„¤ì •ì„ ì €ìž¥í•©ë‹¤.

ì´ì œ RV016, RV042, RV042G ë° RV082 VPN ë¼ìš°í„°ì—ì„œ í´ë¼ì´ì–¸íŠ¸ì—ì„œ ê²Œì´íŠ¸ì›¨ì´ë¡œ ì›ê²© ì•¡ì„¸ìŠ¤ VPN í„°ë„ì´ êµ¬ì„±í•˜ëŠ” ë°©ë²•ì› ìŠµë‹ˆë‹¤.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.