www.axgate.com

IPSEC 연동 가이드

AXGATE
Security and Beyond

설정 내용

1. Security parameter 설정 내용

```
security parameters
 ike version 2 mobike
 ike local-id address [공인 IP Address]
 ike remote-id address [remote 공인 IP Address]
 ike local-psk [preshard key]
 ike remote-psk [preshard key]
 ike proposal encryption aes256 integrity sha1 prf sha1 dh-group 2
 ike timer rekey 20000 dpd 10
 ipsec proposal encryption aes256 integrity sha1
 ipsec lifetime seconds 3600
 qos priority queue length 10
 qos priority queue restore-time 10000
 qos priority queue host-lifetime 60
 nat entry-limit 500
 objects node-limit 5000
 policy node-limit 2500
 reference update-time 600
 routing-cache enable
!
```

** target group ipsec1
proto icmp 3 3 source **[IP address]**
delay state-change up 3 down 3
state host **[체크 할 대상 IP address]**

;; icmp 3 3 : icmp 3초 주기로 체크, 3번 응답이 없으면 target 동작

2. IPSEC Profile 설정 내용

```
ip ipsec profile 1
 ike version 2 mobike
 ike reset target-group ipsec state triggered-to-untriggered interval 10
 ike local-id address [local 공인 IP Address]
 ike remote-id address [remote 공인 IP Address]
 ike lifetime seconds [1-4294967295]
 local-address zone untrust [local 공인 IP Address]
 remote-address zone untrust [remote 공인 IP Address]
 local-subnet [암호화 할 대역]
 remote-subnet [암호화 할 대역]
 proposal ike encryption aes256 integrity sha1 prf sha1 dh-group 2
 proposal ipsec encryption aes256 integrity sha1
 ipsec proto esp mode tunnel
 ipsec setup ike
 ipsec lifetime seconds [1-4294967295]
!

axgate#
```

** ike reset target-group ipsec state triggered-to-untriggered interval 10

- target-group 상태 변경에 따른 IPSEC reset 동작 설정

** interval [초] : target state를 interval 주기로 참고함.
- triggered-to-untriggered : target state가 UP->DOWN으로 될 때 구동
- untriggered-to-untriggered : target state가 DOWN->DOWN으로 될때 구동

설정 내용

3. 방화벽 정책에 IPSEC Profile 설정 적용

```
ip security policy from trust to untrust 10 id 1
 source any
 destination any
 ipsec-profile 1
 tcp-mss 1300
 action pass log
 enable
!
ip security policy from untrust to trust 10 id 2
 source any
 destination any
 ipsec-profile 1
 tcp-mss 1300
 action pass log
 enable
!
```

참고 logging message 변경

```
AXGATE# sho run logging
!
logging
 console kernel off
 memory system severity information   -> debugging로 변경
 memory audit
 memory session
 memory application
 memory ipsec
 memory anti-ddos
 memory ips
 memory anti-spam
 memory anti-virus
 memory sslvpn
 memory userauth
```

IPSEC 연동 확인

2. IPSEC 연동 확인

```
axgate# sho sa ike [phase1단계 터널 정보 확인]
STIME               SPI                VER LOCAL_ADDR              REMOTE_ADDR             PROF_ID      STATUS
2019-02-12 13:16:47 eb0a04cce7e43417  2   [local 공인IP address]      [remote 공인IP address]          1       reauth(6690)

axgate#
axgate# sho sa ike ?
  detail  Detailed informations
  <cr>
axgate#
axgate# sho sa ike detail
STIME               SPI                VER LOCAL_ADDR              REMOTE_ADDR             PROF_ID      STATUS          ENCRYPTION  INTEGRITY DH_GROUP REMOTE_SUBADDR
2019-02-12 13:16:47 eb0a04cce7e43417  2   [local 공인IP address]  [remote 공인IP address]          1       reauth(6690)      aes256          sha1        2      0.0.0.0-255.255.255.25
axgate#
axgate# sho sa ipsec [phase1단계 터널 정보 확인]
STIME               SPI       PROTO LOCAL_ADDR              REMOTE_ADDR             PROF_ID NAT-T STATUS
2019-02-12 16:30:54 a97c4881  50    local 공인IP address]          [remote 공인IP address]          1       no    rekeying(1379)
2019-02-12 16:30:54 15a143    50    [remote 공인IP address]          local 공인IP address]          1       no    rekeying(1379)

axgate#
axgate# sho sa ipsec ?
  detail  Detailed informations
  <cr>

axgate# sho sa ipsec detail
STIME               SPI       PROTO LOCAL_ADDR              REMOTE_ADDR             PROF_ID NAT-T STATUS          P1_ENCRYPTION  P1_INTEGRITY  DH_GROUP  P2_ENCRYPTION
 P2_INTEGRITY
2019-02-12 16:30:54 a97c4881  50    local 공인IP address]          [remote 공인IP address]          1       no    rekeying(1213)    aes256          sha1          2         aes256
sha1
2019-02-12 16:30:54 15a143    50    [remote 공인IP address]          local 공인IP address]          1       no    rekeying(1213)    aes256          sha1          2         aes256
sha1
axgate#
axgate#
axgate#
```

IPSEC 연동 확인

2. IPSEC 정상 연동 시 로그 화면(logging 옵션에서 debug 모드로 진행)

sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (76 bytes)
2019-02-12 16:30:35 charon: DBG 07[NET] received packet: from [remote 공인IP address][500] to local 공인IP address][500] (76 bytes)
2019-02-12 16:30:35 charon: DBG 07[ENC] parsed INFORMATIONAL request 898 [ ]
2019-02-12 16:30:35 charon: DBG 07[ENC] generating INFORMATIONAL response 898 [ ]
2019-02-12 16:30:35 charon: DBG 07[NET] sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (76 bytes)
2019-02-12 16:30:45 charon: DBG 15[NET] received packet: from [remote 공인IP address][500] to local 공인IP address][500] (76 bytes)
2019-02-12 16:30:45 charon: DBG 15[ENC] parsed INFORMATIONAL request 899 [ ]
2019-02-12 16:30:45 charon: DBG 15[ENC] generating INFORMATIONAL response 899 [ ]
2019-02-12 16:30:45 charon: DBG 15[NET] sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (76 bytes)
2019-02-12 16:30:54 charon: DBG 10[IKE] establishing CHILD_SA 1{1}
2019-02-12 16:30:54 charon: DBG 10[ENC] generating CREATE_CHILD_SA request 14 [N(REKEY_SA) N(ESP_TFC_PAD_N) SA No TSi TSr]
2019-02-12 16:30:54 charon: DBG 10[NET] sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (220 bytes)
2019-02-12 16:30:54 charon: DBG 09[NET] received packet: from [remote 공인IP address][500] to local 공인IP address][500] (188 bytes)
2019-02-12 16:30:54 charon: DBG 09[ENC] parsed CREATE_CHILD_SA response 14 [SA No TSi TSr]
2019-02-12 16:30:54 charon: DBG 09[CHD] adding [1] inbound ESP SA : tunnel / 0 [initiator]
2019-02-12 16:30:54 charon: DBG 09[CHD] SPI 0xa97c4881, IPv4 src [remote 공인IP address] dst local 공인IP address]
2019-02-12 16:30:54 charon: DBG 09[CHD] adding SAD entry with SPI a97c4881[a97c4881] and reqid {1}
2019-02-12 16:30:54 charon: DBG 09[CHD] using encryption algorithm AES_CBC(12) with key size 256(256)
2019-02-12 16:30:54 charon: DBG 09[CHD] using integrity algorithm HMAC_SHA1_96(2) with key size 160(0)
2019-02-12 16:30:54 charon: DBG 09[CHD] 0.0.0.0/0 === 192.168.1.0/24
2019-02-12 16:30:54 charon: DBG 09[CHD] subnet [192.168.1.0] === [192.168.1.255]
2019-02-12 16:30:54 charon: DBG 09[CHD] [A] creating rekey job for ESP CHILD_SA with SPI a97c4881 myspi a97c4881and reqid {1} rekey_time{2929}
2019-02-12 16:30:54 charon: DBG 09[CHD] adding [1] outbound ESP SA : tunnel / 0 [initiator]
2019-02-12 16:30:54 charon: DBG 09[CHD] SPI 0x0015a143, IPv4 src local 공인IP address] dst [remote 공인IP address]
2019-02-12 16:30:54 charon: DBG 09[CHD] adding SAD entry with SPI 0015a143[0015a143] and reqid {1}
2019-02-12 16:30:54 charon: DBG 09[CHD] using encryption algorithm AES_CBC(12) with key size 256(256)
2019-02-12 16:30:54 charon: DBG 09[CHD] using integrity algorithm HMAC_SHA1_96(2) with key size 160(0)
2019-02-12 16:30:54 charon: DBG 09[CHD] 192.168.1.0/24 === 0.0.0.0/0
2019-02-12 16:30:54 charon: DBG 09[CHD] subnet [0.0.0.0] === [255.255.255.255]
2019-02-12 16:30:54 charon: DBG 09[IKE] CHILD_SA 1{382} established with SPIs a97c4881_i 0015a143_o and TS 192.168.1.0/24 === 0.0.0.0/0
2019-02-12 16:30:54 charon: DBG 09[IKE] reverse-ruote-injection disabled
2019-02-12 16:30:54 charon: DBG 09[IKE] closing CHILD_SA 1{381} with SPIs 46aec9a2_i (0 bytes) 001043bd_o (0 bytes) and TS 192.168.1.0/24 === 0.0.0.0/0

IPSEC 연동 확인

2. IPSEC 정상 연동 시 로그 화면(logging 옵션에서 debug 모드로 진행) - 계속

2019-02-12 16:30:54 charon: DBG 09[IKE] sending DELETE for ESP CHILD_SA with SPI 46aec9a2
2019-02-12 16:30:54 charon: DBG 09[ENC] generating INFORMATIONAL request 15 [D]
2019-02-12 16:30:54 charon: DBG 09[NET] sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (76 bytes)
2019-02-12 16:30:54 charon: DBG 13[KNL] creating delete job for CHILD_SA ESP/0x46aec9a2/local 공인IP address]
2019-02-12 16:30:54 charon: DBG 09[KNL] creating delete job for CHILD_SA ESP/0x001043bd/[remote 공인IP address]
2019-02-12 16:30:54 charon: DBG 11[JOB] @ Kexpire CHILD_SA ESP/0x46aec9a2/local 공인IP address]
2019-02-12 16:30:54 charon: DBG 09[JOB] @ Kexpire CHILD_SA ESP/0x001043bd/[remote 공인IP address]
2019-02-12 16:30:54 charon: DBG 12[NET] received packet: from [remote 공인IP address][500] to local 공인IP address][500] (76 bytes)
2019-02-12 16:30:54 charon: DBG 12[ENC] parsed INFORMATIONAL response 15 [D]
2019-02-12 16:30:54 charon: DBG 12[IKE] received DELETE for ESP CHILD_SA with SPI 001043bd
2019-02-12 16:30:54 charon: DBG 12[IKE] CHILD_SA closed
2019-02-12 16:30:54 charon: DBG 12[CHD] deleting 0x46aec9a2, myspi 0x46aec9a2, otherspi 0x001043bd, src [remote 공인IP address]
dst local 공인IP address] spi:2731126342 cpi:0 src port:500 dst port:500
2019-02-12 16:30:54 charon: DBG 12[CHD] deleting 0x001043bd, myspi 0x46aec9a2, otherspi 0x001043bd, src local 공인IP address]
dst [remote 공인IP address] spi:3175288832 cpi:0 src port:500 dst port:500
2019-02-12 16:30:54 charon: DBG 12[ENC] generating INFORMATIONAL request 16 [ ]
2019-02-12 16:30:54 charon: DBG 12[NET] sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (76 bytes)
2019-02-12 16:30:54 charon: DBG 11[NET] received packet: from [remote 공인IP address][500] to local 공인IP address][500] (76 bytes)
2019-02-12 16:30:54 charon: DBG 11[ENC] parsed INFORMATIONAL response 16 [ ]
2019-02-12 16:30:54 charon: DBG 11[ENC] generating INFORMATIONAL request 17 [ ]
2019-02-12 16:30:54 charon: DBG 11[NET] sending packet: from local 공인IP address][500] to [remote 공인IP address][500] (76 bytes)
2019-02-12 16:30:54 charon: DBG 13[NET] received packet: from [remote 공인IP address][500] to local 공인IP address][500] (76 bytes)