IPsec VPN Policy Based Site-to-Site VRF

:

IPsec VPN Policy Based Site-to-Site VRF Pre-Shared Key Internet(WAN) (192.168.1.0/24) ESR-1 (172.16.1.0/24) ESR-2.

:

IKE:

: 3des;

: sha1.

IPsec:

: 3des ;

: sha1.

 ESR-1 ESR-2 firewall .

ESR-1:

```
ESR-1# sh running-config
hostname ESR-1

object-group service ISAKMP
  port-range 500
  port-range 4500
exit

object-group network Local_net
  ip prefix 192.168.1.0/24
exit
object-group network Remote_net
  ip prefix 172.16.1.0/24
exit

ip vrf test
exit

security zone untrusted
  ip vrf forwarding test
exit
security zone trusted
  ip vrf forwarding test
exit

interface gigabitethernet 1/0/1
  ip vrf forwarding test
  security-zone untrusted
  ip address 192.0.2.1/30
exit
interface gigabitethernet 1/0/2
  ip vrf forwarding test
  security-zone trusted
  ip address 192.168.1.1/24
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol udp
```

```
    match destination-port ISAKMP
    enable
  exit
  rule 10
    action permit
    match protocol esp
    enable
  exit
  rule 11
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair untrusted trusted
  rule 10
    action permit
    match source-address Remote_net
    match destination-address Local_net
    enable
  exit
exit
security zone-pair trusted untrusted
  rule 10
    action permit
    match source-address Local_net
    match destination-address Remote_net
    enable
  exit
exit

security ike proposal IKE_PROPOSAL
exit

security ike policy IKE_POLICY
  pre-shared-key ascii-text <password>
  proposal IKE_PROPOSAL
exit

security ike gateway IKE_GATEWAY
  ike-policy IKE_POLICY
  local address 192.0.2.1
  local network 192.168.1.0/24
  remote address 198.51.100.1
  remote network 172.16.1.0/24
  mode policy-based
exit

security ipsec proposal IPSEC_PROPOSAL
exit

security ipsec policy IPSEC_POLICY
  proposal IPSEC_PROPOSAL
exit

security ipsec vpn IPSEC_VPN
  mode ike
  ip vrf forwarding test
  ike establish-tunnel route
  ike gateway IKE_GATEWAY
  ike ipsec-policy IPSEC_POLICY
  enable
exit

ip route vrf test 0.0.0.0/0 192.0.2.2
```

ESR-1:

```
ESR-1# sh security ipsec vpn status vrf test IPSEC_VPN
Currently active IKE SA:
    Name:                       IPSEC_VPN
    State:                      Established
    Version:                    v1-only
    Unique ID:                  1
    Local host:                 192.0.2.1
    Remote host:                198.51.100.1
    Role:                       Responder
    Initiator spi:              0x1d0c68c51a7cd2f8
    Responder spi:              0x16ed4123946b0295
    Encryption algorithm:       des
    Authentication algorithm:   sha1
    Diffie-Hellman group:       1
    Established:                1 hour, 46 minutes and 58 seconds ago
    Rekey time:                 1 hour, 46 minutes and 58 seconds
    Reauthentication time:      1 hour, 1 minute and 1 second
    Child IPsec SAs:
        Name:                       IPSEC_VPN-4
        State:                      Installed
        Protocol:                   esp
        Mode:                       Tunnel
        Encryption algorithm:       3des
        Authentication algorithm:   sha1
        Rekey time:                 31 minutes and 2 seconds
        Life time:                  43 minutes and 39 seconds
        Established:                16 minutes and 21 seconds ago
        Traffic statistics:
            Input bytes:            873180
            Output bytes:           873180
            Input packets:          10395
            Output packets:         10395
        -------------------------------------------------------------
```

WAN:

```
15:45:54.719594 a8:f9:4b:aa:b3:53 > a8:f9:4b:aa:38:21, ethertype IPv4 (0x0800), length 150: (tos 0x0, ttl 64,
id 0, offset 0, flags [DF], proto ESP (50), length 136)
    192.0.2.1 > 198.51.100.1: ESP(spi=0xc1413691,seq=0x289c), length 116
15:45:54.719999 a8:f9:4b:aa:38:21 > a8:f9:4b:aa:b3:53, ethertype IPv4 (0x0800), length 150: (tos 0x0, ttl 63,
id 13623, offset 0, flags [none], proto ESP (50), length 136)
    198.51.100.1 > 192.0.2.1: ESP(spi=0xcc487721,seq=0x289c), length 116
15:45:54.720073 a8:f9:4b:aa:38:21 > a8:f9:4b:aa:b3:53, ethertype IPv4 (0x0800), length 98: (tos 0x0, ttl 63, id
64462, offset 0, flags [none], proto ICMP (1), length 84)
    172.16.1.10 > 192.168.1.10: ICMP echo reply, id 16, seq 1, length 64
15:45:54.720611 a8:f9:4b:aa:b3:53 > a8:f9:4b:aa:38:21, ethertype IPv4 (0x0800), length 150: (tos 0x0, ttl 64,
id 0, offset 0, flags [DF], proto ESP (50), length 136)
    192.0.2.1 > 198.51.100.1: ESP(spi=0xc1413691,seq=0x289d), length 116
```

ESR-2:

```
ESR-2# sh running-config
hostname ESR-2

object-group service ISAKMP
  port-range 500
  port-range 4500
exit

object-group network Local_net
  ip prefix 172.16.1.0/24
exit
object-group network Remote_net
  ip prefix 192.168.1.0/24
exit

ip vrf test
```

```
exit

security zone untrusted
  ip vrf forwarding test
exit
security zone trusted
  ip vrf forwarding test
exit

interface gigabitethernet 1/0/1
  ip vrf forwarding test
  security-zone untrusted
  ip address 198.51.100.1/30
exit
interface gigabitethernet 1/0/2
  ip vrf forwarding test
  security-zone trusted
  ip address 172.16.1.1/24
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol udp
    match destination-port ISAKMP
    enable
  exit
  rule 10
    action permit
    match protocol esp
    enable
  exit
  rule 11
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair untrusted trusted
  rule 10
    action permit
    match source-address Remote_net
    match destination-address Local_net
    enable
  exit
exit
security zone-pair trusted untrusted
  rule 10
    action permit
    match source-address Local_net
    match destination-address Remote_net
    enable
  exit
exit
security zone-pair trusted self
  rule 10
    action permit
    match protocol icmp
    enable
  exit
exit

security ike proposal IKE_PROPOSAL
exit

security ike policy IKE_POLICY
  pre-shared-key ascii-text <password>
  proposal IKE_PROPOSAL
exit

security ike gateway IKE_GATEWAY
  ike-policy IKE_POLICY
```

```
  local address 198.51.100.1
  local network 172.16.1.0/24
  remote address 192.0.2.1
  remote network 192.168.1.0/24
  mode policy-based
exit

security ipsec proposal IPSEC_PROPOSAL
exit

security ipsec policy IPSEC_POLICY
  proposal IPSEC_PROPOSAL
exit

security ipsec vpn IPSEC_VPN
  mode ike
  ip vrf forwarding test
  ike establish-tunnel route
  ike gateway IKE_GATEWAY
  ike ipsec-policy IPSEC_POLICY
  enable
exit

ip route vrf test 0.0.0.0/0 198.51.100.2
```

ESR-2:

```
ESR-2#  sh security ipsec vpn status vrf test IPSEC_VPN
Currently active IKE SA:
    Name:                       IPSEC_VPN
    State:                      Established
    Version:                    v1-only
    Unique ID:                  1
    Local host:                 198.51.100.1
    Remote host:                192.0.2.1
    Role:                       Initiator
    Initiator spi:              0x1d0c68c51a7cd2f8
    Responder spi:              0x16ed4123946b0295
    Encryption algorithm:       des
    Authentication algorithm:   sha1
    Diffie-Hellman group:       1
    Established:                1 hour, 55 minutes and 46 seconds ago
    Rekey time:                 1 hour, 55 minutes and 46 seconds
    Reauthentication time:      54 minutes and 22 seconds
    Child IPsec SAs:
        Name:                       IPSEC_VPN-4
        State:                      Installed
        Protocol:                   esp
        Mode:                       Tunnel
        Encryption algorithm:       3des
        Authentication algorithm:   sha1
        Rekey time:                 23 minutes and 37 seconds
        Life time:                  34 minutes and 51 seconds
        Established:                25 minutes and 9 seconds ago
        Traffic statistics:
            Input bytes:            3657024
            Output bytes:           3657024
            Input packets:          43536
            Output packets:         43536
        ------------------------------------------------------------
```