Configuring Security Associations

The first IPSec configuration step is to select a type of security association for your IPSec connection. You must statically configure all specifications for manual SAs, but you can rely on some defaults when you configure an IKE dynamic SA. To configure a security association, see the following sections.

- Configuring Manual SAs on page 1
- Configuring IKE Dynamic SAs on page 2

Configuring Manual SAs

On the ES PIC, you configure a manual security association at the [edit security ipsec security-association *name*] hierarchy level. Include your choices for authentication, encryption, direction, mode, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

```
[edit security]
ipsec {
   security-association  sa-name  {
      description  description;
      manual {
         direction (inbound | outbound | bidirectional) {
            authentication {
               algorithm (hmac-md5-96 | hmac-sha1-96);
               key (ascii-text key | hexadecimal key);
            }
            auxiliary-spi auxiliary-spi;
            encryption {
               algorithm (des-cbc | 3des-cbc);
               key (ascii-text key  | hexadecimal key);
            }
            protocol (ah | esp | bundle);
            spi  spi-value;
         }
      }
      mode (tunnel | transport);
   }
}
```

On the AS and MultiServices PICs, you configure a manual security association at the [edit services ipsec-vpn rule *rule-name*] hierarchy level. Include your choices for authentication, encryption, direction, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

```
[edit services ipsec-vpn]
rule rule-name {
   match-direction (input | output);
   term  term-name  {
      from {
         destination-address  address;
         source-address  address;
      }
```

```
            then {
                backup-remote-gateway address;
                clear-dont-fragment-bit;
                manual {
                    direction (inbound | outbound | bidirectional) {
                        authentication {
                            algorithm (hmac-md5-96 | hmac-sha1-96);
                            key (ascii-text key | hexadecimal key);
                        }
                        auxiliary-spi spi-value;
                        encryption {
                            algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
                            # aes-256-cbc, des-cbc, or 3des-cbc.
                            key (ascii-text key | hexadecimal key);
                        }
                        protocol (ah | bundle | esp);
                        spi spi-value;
                    }
                }
                no-anti-replay;
                remote-gateway  address;
                syslog;
            }
        }
    }
    rule-set  rule-set-name  {
        [ rule  rule-names  ];
    }
```

Configuring IKE Dynamic SAs

On the ES PIC, you configure an IKE dynamic SA at the [edit security ike] and [edit security ipsec] hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. The IKE policy must use the IP address of the remote end of the IPSec tunnel as the policy name. Also, include your choices for IPSec policies and proposals, which include options for authentication, encryption, protocols, Perfect Forward Secrecy (PFS), and IPSec modes. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

```
    [edit security]
    ike {
        proposal ike-proposal-name {
            authentication-algorithm (md5 | sha1);
            authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
            description description;
            dh-group (group1 | group2);
            encryption-algorithm (3des-cbc | des-cbc);
            lifetime-seconds seconds;
        }
        policy ike-peer-address {
            description description;
            encoding (binary | pem);
            identity identity-name;
            local-certificate certificate-filename;
            local-key-pair private-public-key-file;
            mode (aggressive | main);
            pre-shared-key (ascii-text key | hexadecimal key);
            proposals [ proposal-names ];
        }
    }
    ipsec {
        proposal ipsec-proposal-name  {
            authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
            description description;
            encryption-algorithm (3des-cbc | des-cbc);
            lifetime-seconds seconds;
            protocol (ah | esp | bundle);
        }
        policy ipsec-policy-name {
            description description;
            perfect-forward-secrecy {
                keys (group1 | group2);
            }
            proposals [ proposal-names ];
        }
        security-association sa-name {
            description description;
            dynamic {
                ipsec-policy policy-name;
                replay-window-size (32 | 64);
            }
            mode (tunnel | transport);
        }
    }
```

On the AS and MultiServices PICs, you configure an IKE dynamic security association at the [edit services ipsec-vpn ike], [edit services ipsec-vpn ipsec], and [edit services ipsec-vpn rule *rule-name*] hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. Also, include your choices for IPSec policies and proposals, which include options for authentication, encryption, protocols, PFS, and IPSec modes. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

If you choose not to explicitly configure IKE and IPSec policies and proposals on the AS and MultiServices PICs, your configuration can default to some preset values. These default values are shown in Table 1.

Table 1: IKE and IPSec Proposal and Policy Default Values for the AS and MultiServices PICs

IKE Policy Statement	Default Value
mode	main
proposals	default
IKE Proposal Statement	Default Value

Table 1: IKE and IPSec Proposal and Policy Default Values for the AS and MultiServices PICs *(continued)*

IKE Policy Statement	Default Value
authentication-algorithm	sha1
authentication-method	pre-shared-keys
dh-group	group2
encryption-algorithm	3des-cbc
lifetime-seconds	3600 (seconds)
IPSec Policy Statement	Default Value
perfect-forward-secrecy keys	group2
proposals	default
IPSec Proposal Statement	Default Value
authentication-algorithm	hmac-sha1-96
encryption-algorithm	3des-cbc
lifetime-seconds	28800 (seconds)
protocol	esp

NOTE: If you use the default IKE and IPSec policy and proposal values preset within the AS and MultiServices PICs, you must explicitly configure an IKE policy and include a preshared key. This is because the pre-shared-keys authentication method is one of the preset values in the default IKE proposal.

If you decide to configure values manually, the following information shows the complete statement hierarchy and options for dynamic IKE SAs on the AS and MultiServices PICs:

```
[edit services ipsec-vpn]
ike {
   proposal proposal-name {
      authentication-algorithm (md5 | sha1 | sha256);
      authentication-method (pre-shared-keys | rsa-signatures);
      description description;
      dh-group (group1 | group2);
      encryption-algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
      # aes-256-cbc, des-cbc, or 3des-cbc.
      lifetime-seconds seconds;
   }
   policy policy-name {
        description description;
        local-id {
            ipv4_addr [ values ];
            key_id [ values ];
        }
        local-certificate certificate-id-name;
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposals [ proposal-names ];
        remote-id {
            ipv4_addr [ values ];
            key_id [ values ];
        }
    }
}
ipsec {
    proposal proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        description description;
        encryption-algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
        # aes-256-cbc, des-cbc, or 3des-cbc.
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    policy policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
}
rule rule-name {
    match-direction (input | output);
    term term-name {
        from {
            destination-address address;
            source-address address;
        }
        then {
            backup-remote-gateway address;
            clear-dont-fragment-bit;
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            no-anti-replay;
            remote-gateway address;
            syslog;
        }
    }
}
rule-set rule-set-name {
    [ rule rule-names ];
```

```
}
```

Published: 2010-04-15