



I parametri debbono rispondere ai seguenti step di configurazione:

- LOCAL SITE:
 - local IP private network:
 - public network zone:
 - public network interface:
 - tunnel zone:
 - tunnel interface:
 - tunnel IP interface:

- REMOTE SITE:
 - remote IP address public router's:
 - remote IP private network:

Esempio:

Remote Endpoint : 192.168.0.0/28

Local Endpoint : 10.10.10.0/24

Phase 1 : AES-256,SHA1, DH2

Phase 2 : ESP, SHA1, AES-256

TUNNEL INTERFACE

set interfaces st0 unit y family inet

set security zones security-zone untrust-vpn interfaces st0.y

ROUTE

set routing-options static route 192.168.0.0/28 next-hop st0.y

PROPOSALS

set security ike proposal IKE-DH2-AES256-SHA1 authentication-method pre-shared-keys

set security ike proposal IKE-DH2-AES256-SHA1 dh-group group2

set security ike proposal IKE-DH2-AES256-SHA1 authentication-algorithm sha1

set security ike proposal IKE-DH2-AES256-SHA1 encryption-algorithm aes-256-cbc

set security ike proposal IKE-DH2-AES256-SHA1 lifetime-seconds 3600

set security ipsec proposal IPSEC-ESP-AES256-SHA1 protocol esp

set security ipsec proposal IPSEC-ESP-AES256-SHA1 authentication-algorithm hmac-sha1-96

set security ipsec proposal IPSEC-ESP-AES256-SHA1 encryption-algorithm aes-256-cbc

set security ipsec proposal IPSEC-ESP-AES256-SHA1 lifetime-seconds 3600

PHASE 1

set security ike policy IKE-POLICY-SITEA mode main

set security ike policy IKE-POLICY-SITEA proposals IKE-DH2-AES256-SHA1

set security ike policy IKE-POLICY-SITEA pre-shared-key ascii-text <PRESHARED KEY>

set security ike gateway IKE-PEER-SITEA ike-policy IKE-POLICY-SITEA

set security ike gateway IKE-PEER-SITEA address <PEER IP>

set security ike gateway IKE-PEER-SITEA external-interface rethx.y

PHASE 2

set security ipsec policy IPSEC-POLICY proposals IPSEC-ESP-AES256-SHA1

set security ipsec vpn VPN-SITEA bind-interface st0.y

set security ipsec vpn VPN-SITEA ike gateway IKE-PEER-SITEA

set security ipsec vpn VPN-SITEA ike ipsec-policy IPSEC-POLICY

set security ipsec vpn VPN-SITEA establish-tunnels immediately

POLICY

set security zones security-zone untrust-vpn address-book address 192.168.0.0/28 192.168.0.0/28

set security zones security-zone trust address-book address 10.10.10.0/24 10.10.10.0/24

set security policies from-zone trust to-zone untrust-vpn policy trust-untrust-vpn match source-address 10.10.10.0/24

set security policies from-zone trust to-zone untrust-vpn policy trust-untrust-vpn match destination-address 192.168.0.0/28

set security policies from-zone trust to-zone untrust-vpn policy trust-untrust-vpn match application any

set security policies from-zone trust to-zone untrust-vpn policy trust-untrust-vpn then permit

set security policies from-zone untrust-vpn to-zone trust policy untrust-trust-vpn match source-address 192.168.0.0/28

set security policies from-zone untrust-vpn to-zone trust policy untrust-trust-vpn match destination-address 10.10.10.0/24

set security policies from-zone untrust-vpn to-zone trust policy untrust-trust-vpn match application any

set security policies from-zone untrust-vpn to-zone trust policy untrust-trust-vpn then permit