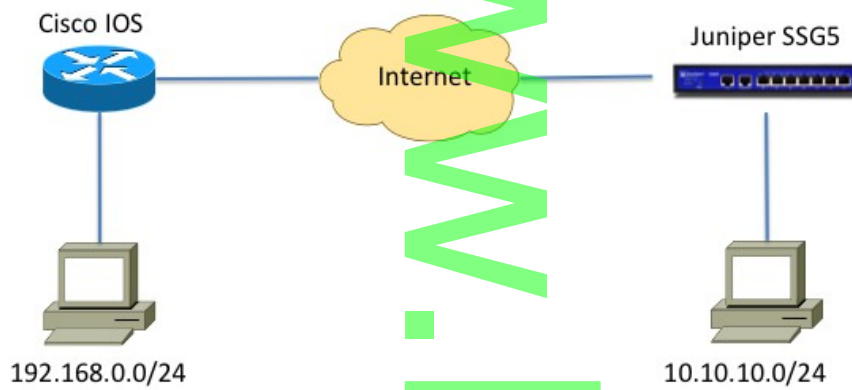


IPSec VPN Site-to-Site Juniper SSG5 to Cisco IOS



Phase 1

- pre-shared key 112233
- DH Group2
- Encryption 3DES
- Hash MD5
- Lifetime 28800
- Main mode
- Enable NAT-T

Phase 2

- No PFS
- ESP 3DES MD5
- Lifetime 3600

www.boornsee.net

[Juniper SSG5]

```
set admin password <PASSWORD>
set interface ethernet0/0 ip 103.3.176.86/30
set interface ethernet0/0 ip manageable
set interface ethernet0/0 manage ping
set interface ethernet0/0 manage ssh
set interface ethernet0/0 manage telnet
set interface ethernet0/0 manage web
set route 0.0.0.0/0 gateway 103.3.176.85
```

The screenshot displays the Juniper SSG5-Serial configuration interface. The top navigation bar includes 'Home', 'sbg5-serial', and a help icon. The main content area is divided into several sections:

- My ssg5-serial:** Hardware Version: 710(0), Firmware Version: 6.2.0r6.0 (Firewall+VPN), Serial Number: 0162032010002070, Host Name: ssg5-serial.
- System Status (Root):** Administrator: netscreen, Current Logins: 1.
- Chassis Summary:** Resources Status section with progress bars for CPU, Memory, Sessions, and Policies.
- Interface / VPN Link Status Monitoring:** A table showing resource status.
- System Most Recent Alarms / Events:** Two empty tables for alarms and events.

Resource	Total	Up	Down	Unused/Inactive	Details
Physical Interface	12	1	11	4	Go to interface list
IPSec VPN	1	0	0	1	Go to VPN Monitor

Date/Time	Level	Description
No entry available.		

Date/Time	Level	Description
2013-09-05		

Vertical watermark: www.b00nnee.net

Network > Interfaces (List) ssg5-serial ?

List 20 per page

List ALL(8) Interfaces New Tunnel IF

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Down	-	Edit
ethernet0/2				Down	-	Edit
ethernet0/3				Down	-	Edit
ethernet0/4				Down	-	Edit
ethernet0/5				Down	-	Edit
ethernet0/6				Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	103.3.176.86/30	Untrust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Network > Interfaces > Edit ssg5-serial ?

Interface: ethernet0/0 (IP/Netmask: 103.3.176.86/30) [Back To Interface List](#)

Properties: [Basic](#) [Phy](#) [MIP](#) [DIP](#) [VIP](#) [IGMP](#) [Monitor](#) [802.1X](#) [IRDP](#)

Interface Name ethernet0/0 2c6b.f51d.5440

Zone Name Untrust

Obtain IP using DHCP Automatic update DHCP server parameters
 Obtain IP using PPPoE [Create new pppoe setting](#)
 Static IP

IP Address / Netmask 103.3.176.86 / 30 Manageable

Manage IP * 103.3.176.86 2c6b.f51d.5440

Interface Mode NAT Route

Block Intra-Subnet Traffic

Service Options

Management Services Web UI Telnet SSH
 SNMP SSL

Other Services Ping Path MTU(IPv4) Ident-reset

Maximum Transfer Unit(MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy

NTP Server

WebAuth IP Address 0.0.0.0 SSL Only

G-ARP

Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps
 Ingress Maximum Bandwidth 0 Kbps

www.powers.net

VPNs > AutoKey Advanced > Gateway > Edit ssg5-serial ?

Juniper NETWORKS
SSG5-Serial

Home
Configuration
Network
Binding
DNS
Zones
Interfaces
List
Backup
DHCP
802.1X
Routing
PPP
Security
Policy
VPNs
AutoKey IKE
AutoKey Advanced
Gateway
P1 Proposal
P2 Proposal
XAuth Settings
VPN Groups
Manual Key
L2TP
Monitor Status

Gateway Name: VPN1
Version: IKEv1 IKEv2

Remote Gateway
 Static IP Address IP Address/Hostname: 61.90.191.98
 Dynamic IP Address Peer ID:
 Dialup User User: None
 Dialup User Group Group: None

ACVPN-Dynamic Local ID:
 ACVPN-Profile

OK Cancel **Advanced** Click

VPNs > AutoKey Advanced > Gateway > Edit ssg5-serial ?

Juniper NETWORKS
SSG5-Serial

Home
Configuration
Network
Binding
DNS
Zones
Interfaces
List
Backup
DHCP
802.1X
Routing
PPP
Security
Policy
VPNs
AutoKey IKE
AutoKey Advanced
Gateway
P1 Proposal
P2 Proposal
XAuth Settings

IKEv2 Auth Method
Self: None Peer: None

Preshared Key: Use As Seed:
Local ID: (optional)

Outgoing Interface: ethernet0/0

Security Level: Predefined Standard Compatible Basic
User Defined: Custom

Phase 1 Proposal: pre-g2-3des-md5 None None None

Mode (Initiator): Main (ID Protection) Aggressive

Enable NAT-Traversal
UDP Checksum:
Keepalive Frequency: 5 Seconds (0~300)

Peer Status Detection
 Heartbeat
Hello: 0 Seconds (1~3600, 0: disable)
Reconnect: 0 Seconds (60~9999, 0: default)
Threshold: 5 (2~9999)
 DPD
Interval: 0 Seconds (3~28800, 0: disable)
Retry: 5 (1~127)

VPNs > AutoKey IKE > Edit ssg5-serial ?

Juniper NETWORKS
SSG5-Serial

Home
Configuration
Network
Binding
DNS
Zones
Interfaces
List
Backup
DHCP
802.1X
Routing
PPP
Security
Policy
VPNs
AutoKey IKE
AutoKey Advanced
Gateway
P1 Proposal
P2 Proposal
XAuth Settings
VPN Groups
Manual Key
L2TP
Monitor Status

VPN Name: VPN1

Remote Gateway Create a Simple Gateway

Gateway Name: VPN1
Version: IKEv1 IKEv2
Type: Static IP Address/Hostname:
 Dynamic IP Peer ID:
 Dialup User User: None
 Dialup Group Group: None

Local ID: (optional)
Preshared Key: Use As Seed:
Security Level: Standard Compatible Basic
Outgoing Interface: ethernet0/0

ACVPN-Dynamic Gateway: None Tunnel Towards Hub:
 ACVPN-Profile Binding to Tunnel: None

OK Cancel **Advanced** Click

VPNs > AutoKey IKE > Edit ssg5-serial ?

Juniper NETWORKS

SSG5-Serial

- Home
- Configuration
- Network
 - Binding
 - DNS
 - Zones
 - Interfaces
 - List
 - Backup
 - DHCP
 - 802.1X
 - Routing
 - PPP
- Security
- Policy
- VPNs
 - AutoKey IKE
 - AutoKey Advanced
 - Gateway
 - P1 Proposal
 - P2 Proposal
 - XAuth Settings
 - VPN Groups
 - Manual Key
 - L2TP
 - Monitor Status

Security Level

Predefined Standard Compatible Basic
 User Defined Custom

Phase 2 Proposal
 nopfs-esp-3des-md5 / None / None / None

Replay Protection
 Transport Mode

Bind to None Tunnel Interface Tunnel Zone
 none / Untrust-Tun

Proxy-ID
 Local IP / Netmask / /
 Remote IP / Netmask / /
 Service ANY

DSCP Marking Disable Enable Dscp Value 0

VPN Group None Weight 0

VPN Monitor
 Source Interface default
 Destination IP default
 Optimized
 Rekey

Return Cancel

Policy > Policies (From Trust To Untrust) ssg5-serial ?

Juniper NETWORKS

SSG5-Serial

- Home
- Configuration
- Network
- Security
- Policy
 - Policies
 - MCast Policies
 - Policy Elements
- VPNs
- Objects
- Reports
- Wizards
- Help
- Logout

Name (optional) 192.168.0.0

Source Address New Address / / Address Book Entry 10.10.10.0/24 Multiple

Destination Address New Address / / Address Book Entry 192.168.0.0/24 Multiple

Service ANY Multiple
 Application None

WEB Filtering

Action Tunnel Deep Inspection

Tunnel VPN VPN1
 Modify matching bidirectional VPN policy

L2TP None

Logging at Session Beginning

Session-limit
 Counter 0

Alarm without drop

OK Cancel Advanced

Policy > Policies (From Untrust To Trust) ssg5-serial ?

Juniper NETWORKS

SSG5-Serial

- Home
- Configuration
- Network
- Security
- Policy
 - Policies
 - MCast Policies
 - Policy Elements
- VPNs
- Objects
- Reports
- Wizards
- Help
- Logout

Name (optional) 192.168.0.0

Source Address New Address / / Address Book Entry 192.168.0.0/24 Multiple

Destination Address New Address / / Address Book Entry 10.10.10.0/24 Multiple

Service ANY Multiple
 Application None

WEB Filtering

Action Tunnel Deep Inspection

Tunnel VPN VPN1
 Modify matching bidirectional VPN policy

L2TP None

Logging at Session Beginning

Session-limit
 Counter 0

Alarm without drop

OK Cancel Advanced

Policy > Policies (From All zones To All zones) ssg5-serial ?

List per page Search

From To

From Trust To Untrust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
3	10.10.10.0/24	192.168.0.0/24	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	
1	Any	Any	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
2	192.168.0.0/24	10.10.10.0/24	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

Juniper NETWORKS

SSG5-Serial

- [Home](#)
- [Configuration](#)
- [Network](#)
- [Security](#)
- [Policy](#)
 - [Policies](#)
 - [MCast Policies](#)
 - [Policy Elements](#)
- [VPNs](#)
- [Objects](#)
- [Reports](#)
- [Wizards](#)
- [Help](#)
- [Logout](#)

Reports > System Log > Event ssg5-serial ?

List per page Search

Date / Time	Level	Description
2013-09-05 23:06:38	info	IKE 61.90.191.98 Phase 2 msg ID 0802f046: Completed negotiations with SPI 7d0636c5, tunnel ID 1, and lifetime 3600 seconds/4194303 KB.
2013-09-05 23:06:38	info	IKE 61.90.191.98 phase 2:The symmetric crypto key has been generated successfully.
2013-09-05 23:06:38	info	IKE 61.90.191.98 Phase 2 msg ID d802f046: Responded to the peer's first message.
2013-09-05 23:06:38	info	IKE 61.90.191.98: Received initial contact notification and removed Phase 1 SAs.
2013-09-05 23:06:38	info	IKE 61.90.191.98 Phase 1: Completed Main mode negotiations with a 28800-second lifetime.
2013-09-05 23:06:38	info	IKE 61.90.191.98: Received initial contact notification and removed Phase 2 SAs.
2013-09-05 23:06:38	info	IKE 61.90.191.98: Received a notification message for DOI 1 24578 INITIAL-CONTACT.
2013-09-05 23:06:38	info	IKE 61.90.191.98 phase 1:The symmetric crypto key has been generated successfully.
2013-09-05 23:06:38	info	IKE 61.90.191.98 Phase 1: Responder starts MAIN mode negotiations.
2013-09-05 23:06:20	notif	All logged events or alarms were cleared by admin netscreen

Juniper NETWORKS

SSG5-Serial

- [Home](#)
- [Configuration](#)
- [Network](#)
- [Security](#)
- [Policy](#)
 - [Policies](#)
 - [MCast Policies](#)
 - [Policy Elements](#)
- [VPNs](#)
- [Objects](#)
- [Reports](#)
 - [System Log](#)
 - [Event](#)
 - [Self](#)
 - [Asset Recovery](#)
 - [Counters](#)
 - [Chassis](#)
 - [Interface Bandwidth](#)
 - [Policies](#)
 - [Administrator Login](#)
 - [MacAddress](#)
 - [Active Users](#)
- [Wizards](#)
- [Help](#)
- [Logout](#)

```
[Cisco]
ip access-list extended VPN
 permit ip 192.168.0.0 0.0.0.255 10.10.10.0 0.0.0.255

crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 112233 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set JUNIPER-SSG5 esp-3des esp-md5-hmac
crypto map JUNIPER-SSG5 10 ipsec-isakmp
 set peer 103.3.176.86
 set transform-set JUNIPER-SSG5
 match address VPN

interface vlan10
 description ## Internet ##
 ip address 61.90.191.98 255.255.255.252
 crypto map JUNIPER-SSG5

Cisco#sh crypto ipsec sa

interface: Vlan10
 Crypto map tag: JUNIPER-SSG5, local addr 61.90.191.98

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer 103.3.176.86 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

local crypto endpt.: 61.90.191.98, remote crypto endpt.: 103.3.176.86
path mtu 1500, ip mtu 1500
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

Cisco#ping 10.10.10.1 source lo200

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.0.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 4/5/8 ms

Cisco#sh crypto ipsec sa

interface: Vlan10

Crypto map tag: JUNIPER-SSG5, local addr 61.90.191.98

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)

current_peer 103.3.176.86 port 500

PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 61.90.191.98, remote crypto endpt.: 103.3.176.86

path mtu 1500, ip mtu 1500
current outbound spi: 0x7D0636C5(2097559237)

inbound esp sas:

spi: 0x123D8D58(306023768)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
conn id: 15, flow_id: C87X_MBRD:15, crypto map: JUNIPER-SSG5
sa timing: remaining key lifetime (k/sec): (4392926/3595)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

spi: 0x7D0636C5(2097559237)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
conn id: 16, flow_id: C87X_MBRD:16, crypto map: JUNIPER-SSG5
sa timing: remaining key lifetime (k/sec): (4392926/3595)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcsp sas:

www.boornsee.net