Configuration Guide

How to set up the IPSec site-to-site Tunnel between the D-Link DSR Router and the Cisco Firewall

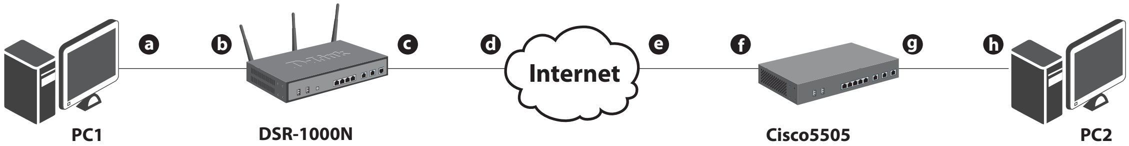
Overview

This document describes how to implement IPSec with pre-shared secrets establishing site-to-site VPN tunnel between the D-Link DSR-1000N and the Cisco 5505. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 8.0(4) of Cisco 5505. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

D-Link®

Situation note

Site-to-site VPN could be implemented in an enterprise allows to access and exchange data among more than two geographical sites or offices. Once the site-to-site VPN set up, the clients in the groups of the different located sites are as in the internal networks. As companies may have other gateway appliances which are not D-Link products, this document will be useful when you intend to create IPSec VPN tunnel between DSR and other existing gateway appliance.



a 192.168.10.100/24
b 192.168.10.1/24 (LAN 1)
c 1.1.1.2/30 (WAN1)

d 1.1.1.2/30
e 2.2.2.1/30

f 2.2.2.1/30 (eth0/7)
g 192.168.1.1/24 (eth0/0)
h 192.168.1.100/24

IP addresses

DSR WAN: **1.1.1.2/30**
DSR LAN: **192.168.10.1/24**

Cisco5505 WAN: **2.2.2.2/30**
Cisco5505 LAN: **192.168.1.1/24**

IPSec Parameters

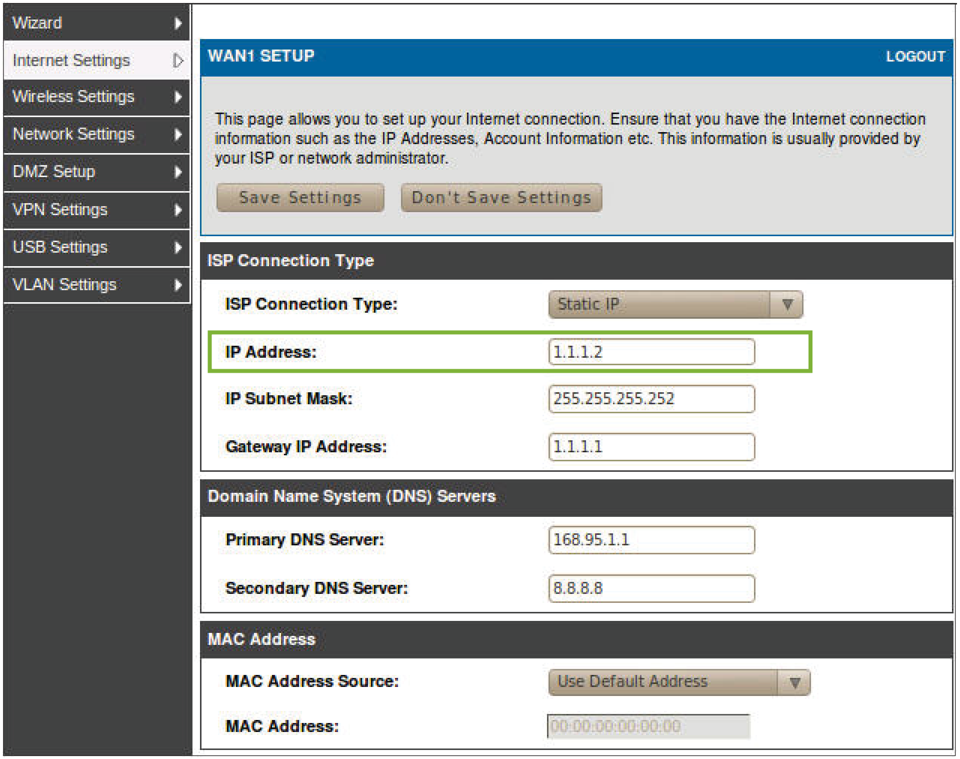
IPSec Mode: **Tunnel Mode**
IPSec Protocol: **ESP**
Phase1 Exchange Mode: **Main**
Phase1 Encryption: **3DES**
Phase1 Authentication: **SHA1**
Phase1 Authentication Method: **Pre-Shared Key**

Diffie-Hellman Group: **G2**
Phase1 Lifetime: **28800 sec**
Phase2 Encryption: **3DES**
Phase2 Authentication: **SHA1**
Phase2 Lifetime: **3600 sec**

Configuration Step

DSR Settings

1. Set up the WAN IP address. Navigate to the Internet Settings > WAN1 Settings > WAN1 Setup.
Fill in relative information based on the settings of topology. The **IP Address** of the field of ISP Connection Type is the IP address of external network connecting point which is shown as the point "**c**" on the topology. Click the button "**save settings**" to complete WAN IP address settings.



This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

ISP Connection Type

ISP Connection Type: Static IP
IP Address: 1.1.1.2
IP Subnet Mask: 255.255.255.252
Gateway IP Address: 1.1.1.1

Domain Name System (DNS) Servers

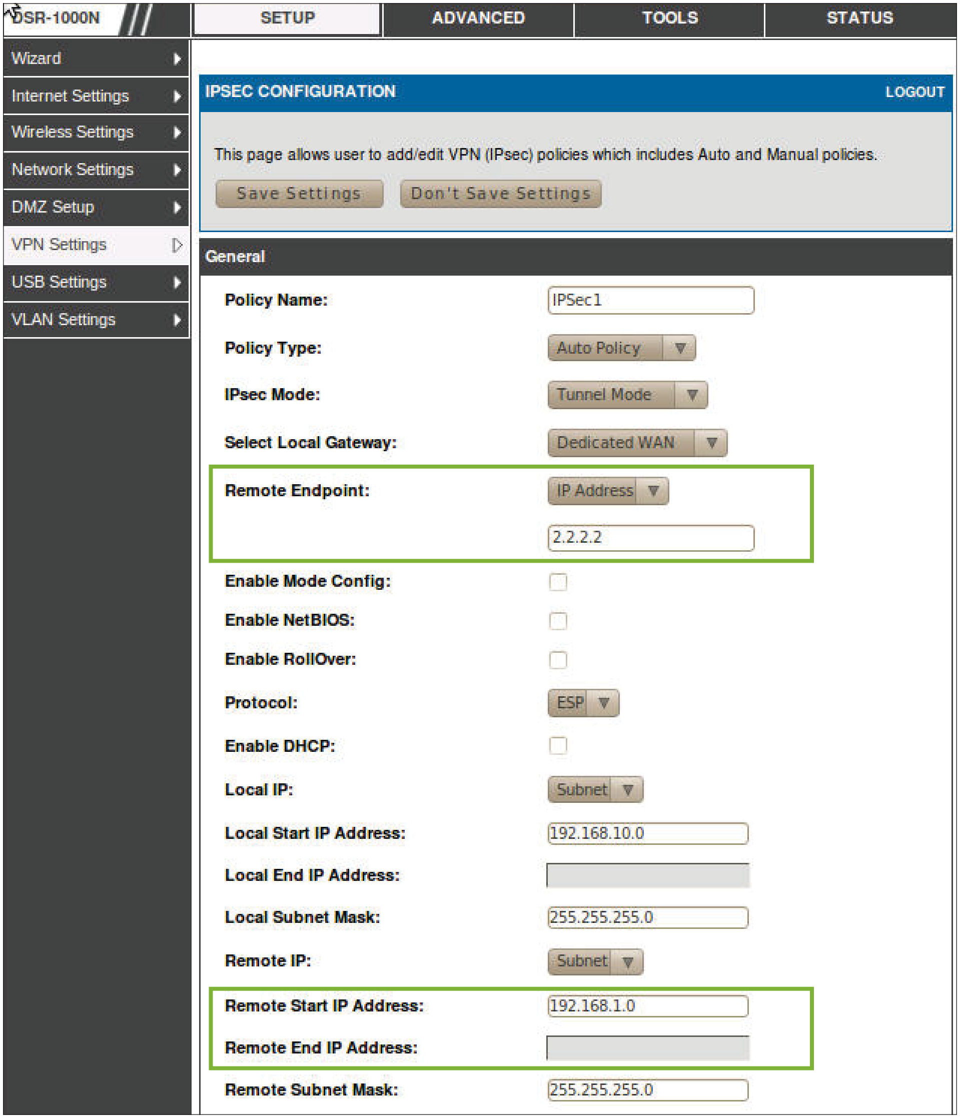
Primary DNS Server: 168.95.1.1
Secondary DNS Server: 8.8.8.8

MAC Address

MAC Address Source: Use Default Address
MAC Address: 00:00:00:00:00:00

2. Set up the IPSec policy. Navigate to the VPN Settings > IPSec > IPSec Policies.

Press the button "**Add**" to increase a new policy. In General Section, fill in relative information. The IP address of **Remote Endpoint** refers to the external network connecting point of Cisco 5505 which is shown as the point "**f**" on the topology. The internal network group, which is indicates the IP information on **Local Start IP Address**, under DSR-1000N allows access to the remote network group, which is indicates the IP information on **Remote Start IP Address**, under Cisco 5505 through VPN tunnel.

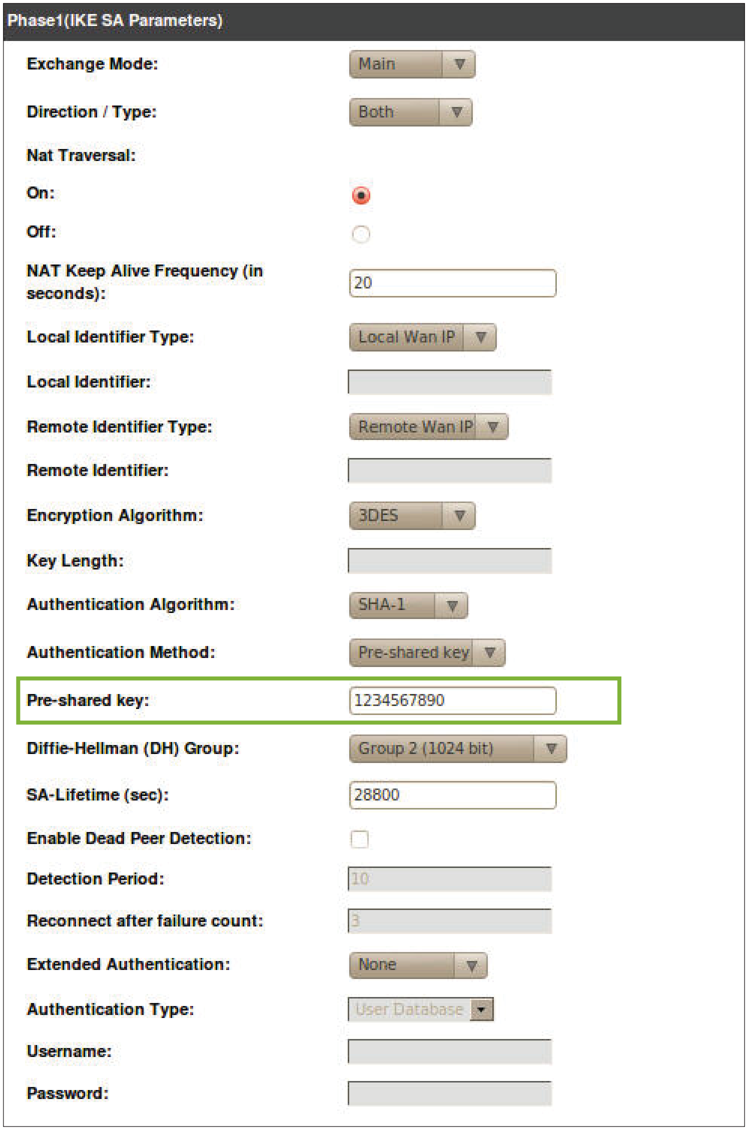


This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.

General

Policy Name:	IPSec1
Policy Type:	Auto Policy
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address 2.2.2.2
Enable Mode Config:	□
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Remote IP:	Subnet
Remote Start IP Address:	192.168.1.0
Remote End IP Address:	
Remote Subnet Mask:	255.255.255.0

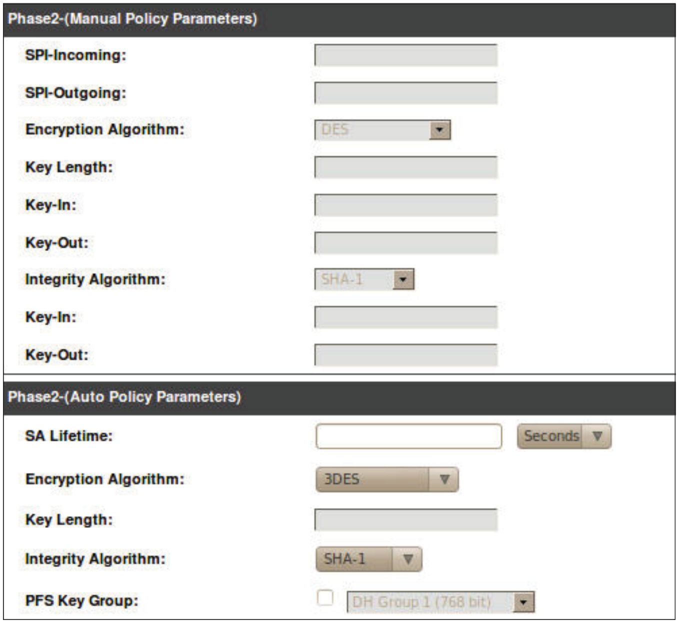
In Phase 1 Section, fill in relative information. Please notice that the **Pre-shared Key** must be as same as the pre-shared key which will be inserted on Cisco 5505 on the later step.



Phase1(IKE SA Parameters)

Exchange Mode:	Main ▼
Direction / Type:	Both ▼
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP ▼
Local Identifier:	
Remote Identifier Type:	Remote Wan IP ▼
Remote Identifier:	
Encryption Algorithm:	3DES ▼
Key Length:	
Authentication Algorithm:	SHA-1 ▼
Authentication Method:	Pre-shared key ▼
Pre-shared key:	1234567890
Diffie-Hellman (DH) Group:	Group 2 (1024 bit) ▼
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None ▼
Authentication Type:	User Database ▼
Username:	
Password:	

In Phase 2 Section, fill in relative information.



Phase2-(Manual Policy Parameters)

SPI-Incoming:	
SPI-Outgoing:	
Encryption Algorithm:	DES
Key Length:	
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1
Key-In:	
Key-Out:	

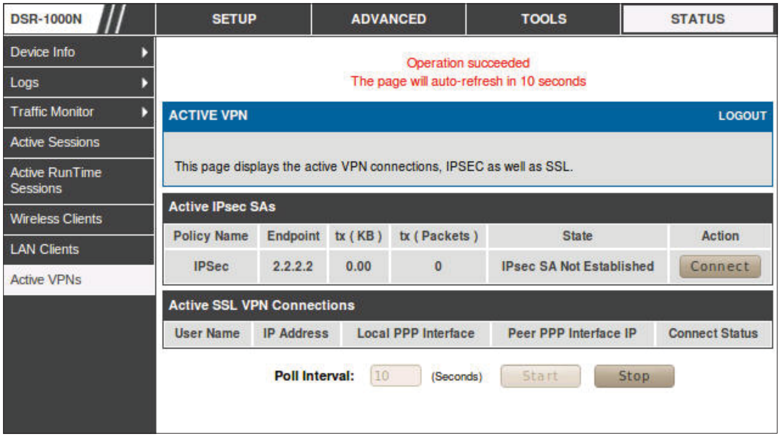
Phase2-(Auto Policy Parameters)

SA Lifetime:	Seconds
Encryption Algorithm:	3DES
Key Length:	
Integrity Algorithm:	SHA-1
PFS Key Group:	□ DH Group 1 (768 bit)

Click the button "**save settings**" to complete IPSec Policy settings.

3. Check the VPN status. Navigate to the Status > Active VPNs.

The activity will be shown on the list while the tunnel is established with the other side.



Operation succeeded
The page will auto-refresh in 10 seconds

ACTIVE VPN

This page displays the active VPN connections, IPSEC as well as SSL.

Active IPsec SAs

Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action
IPSec	2.2.2.2	0.00	0	IPsec SA Not Established	Connect

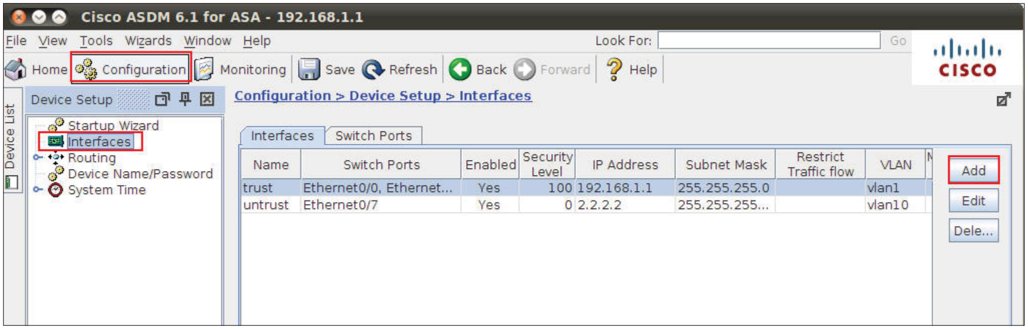
Active SSL VPN Connections

User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status

Poll Interval: 10 (Seconds) Start Stop

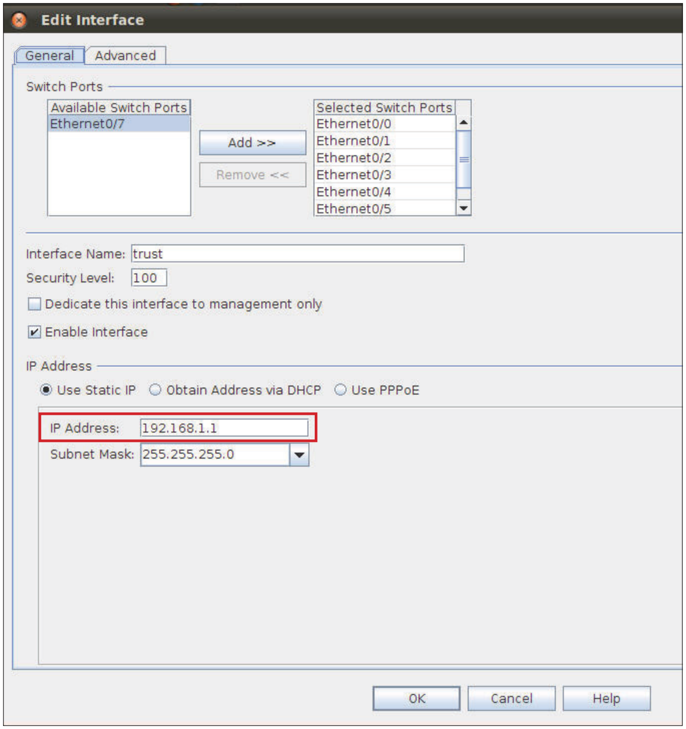
Cisco5505 Settings

1. Set up the Internal and External IP addresses. Navigate to the Configuration > Device Setup > Interfaces. Press button "**Add**" to increase two new interfaces.


Cisco ASDM 6.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For: Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Setup
Startup Wizard
Interfaces
Routing
Device Name/Password
System Time
Configuration > Device Setup > Interfaces
Interfaces Switch Ports
Add
Edit
Dele...

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask	Restrict Traffic flow	VLAN
trust	Ethernet0/0, Ethernet...	Yes	100	192.168.1.1	255.255.255.0		vlan1
untrust	Ethernet0/7	Yes	0	2.2.2.2	255.255.255...		vlan10

First, edit the trust interface. Select and fill in relative information as below. The **IP Address** of General tab is the IP address of internal network connecting point which is shown as the point "g" on the topology. Click the button "**OK**" to complete this setting.



Available Switch Ports	Selected Switch Ports
Ethernet0/7	Ethernet0/0
	Ethernet0/1
	Ethernet0/2
	Ethernet0/3
	Ethernet0/4
	Ethernet0/5

Interface Name: trust

Security Level: 100

☐ Dedicate this interface to management only

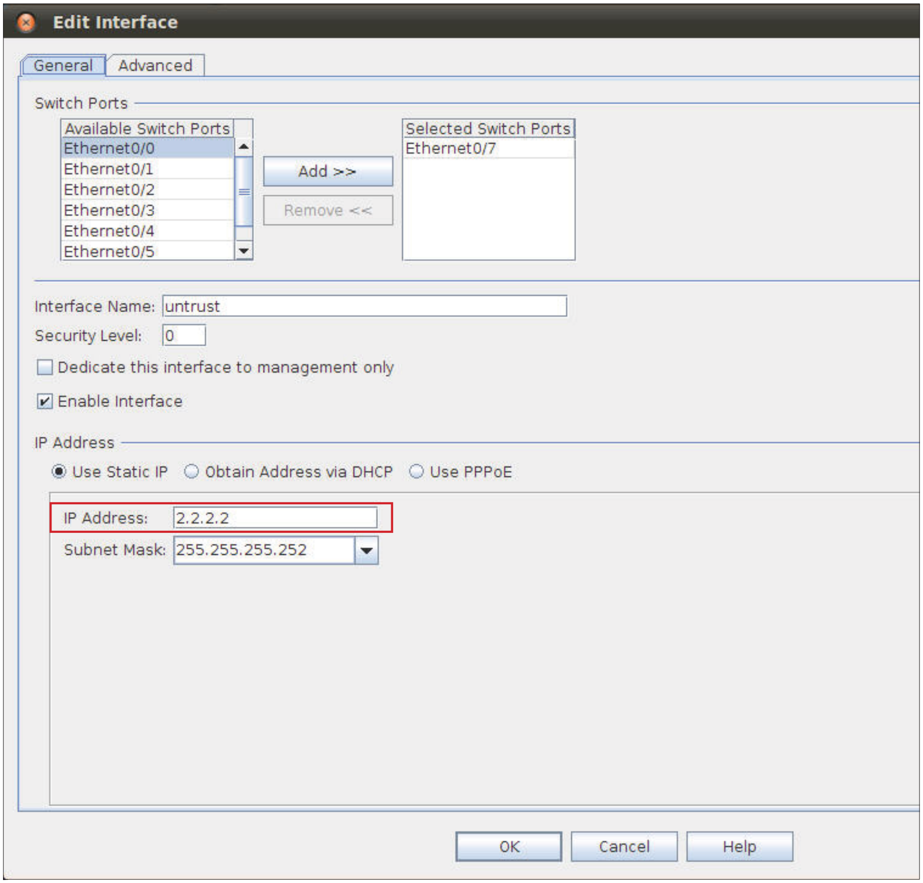
☑ Enable Interface

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Second, edit the untrust interface. Select and fill in relative information as below. The **IP Address** of General tab is the IP address of external network connecting point which is shown as the point "**f**" on the topology. Click the button "**OK**" to complete this setting.



Available Switch Ports: Ethernet0/0, Ethernet0/1, Ethernet0/2, Ethernet0/3, Ethernet0/4, Ethernet0/5

Selected Switch Ports: Ethernet0/7

Interface Name: untrust

Security Level: 0

□ Dedicate this interface to management only

☑ Enable Interface

IP Address

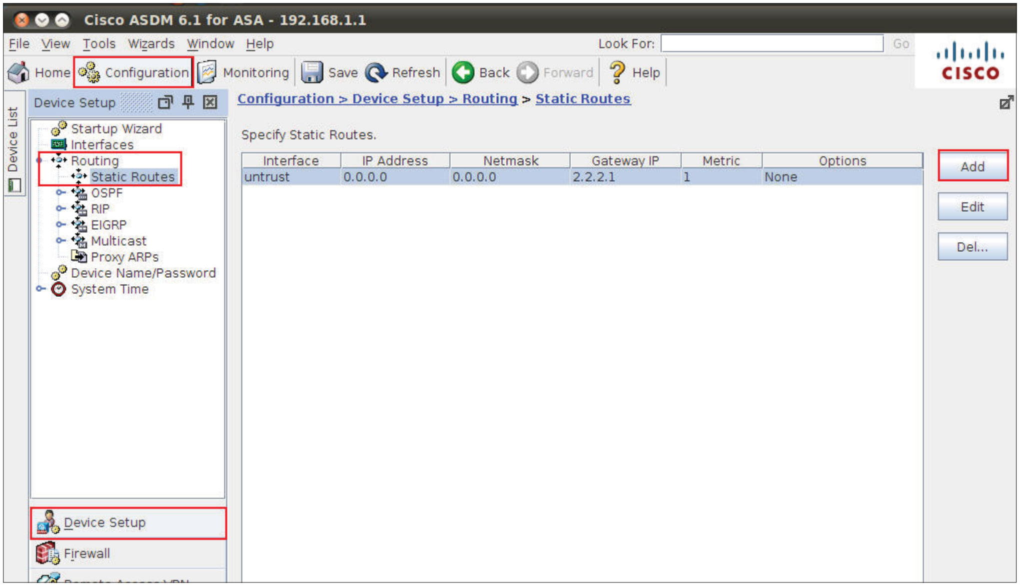
● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 2.2.2.2

Subnet Mask: 255.255.255.252

2. Set up the default gateway. Navigate to Configuration > Device Setup > Routing > Static Routes.

Press the button "**Add**".

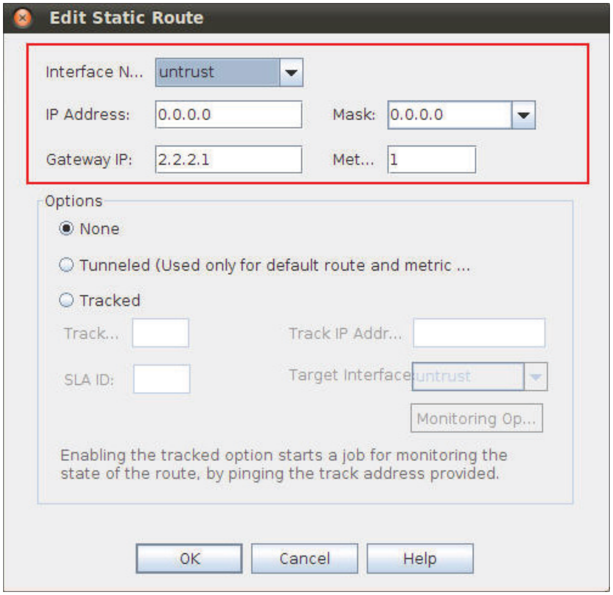


Configuration > Device Setup > Routing > Static Routes

Specify Static Routes.

Interface	IP Address	Netmask	Gateway IP	Metric	Options
untrust	0.0.0.0	0.0.0.0	2.2.2.1	1	None

Select untrust interface as the default gateway interface. Fill in relative information as below.



Interface N...: untrust

IP Address: 0.0.0.0 Mask: 0.0.0.0

Gateway IP: 2.2.2.1 Met...: 1

● None

○ Tunneled (Used only for default route and metric ...

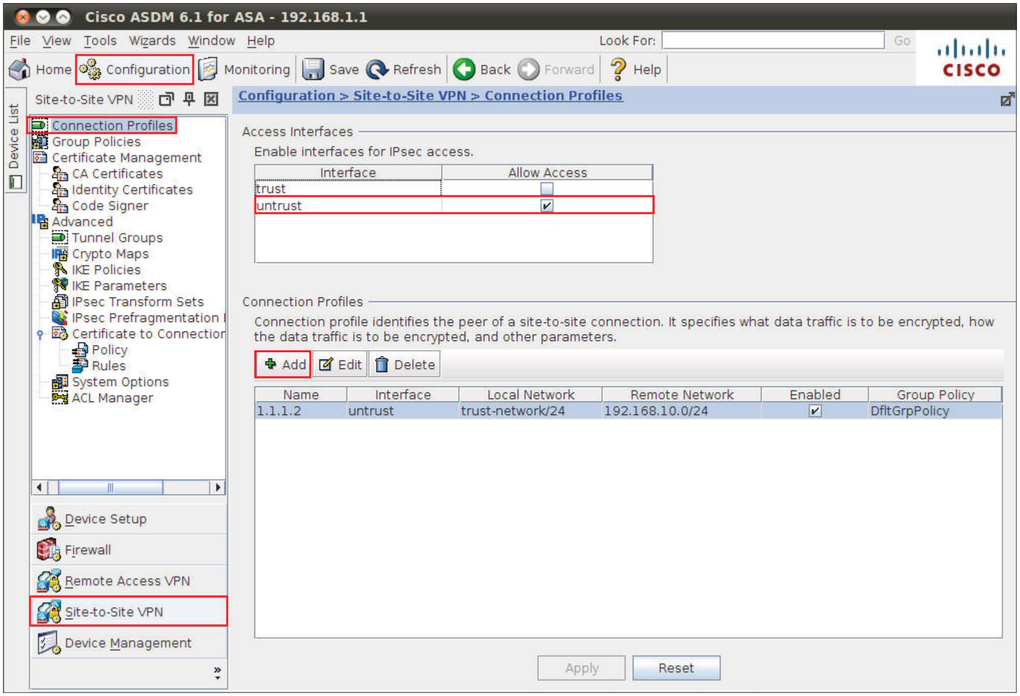
○ Tracked

Target Interface: untrust

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

3. Set up the IPSec Tunnel. Navigate to the Configuration > Site-to-Site VPN > Connection Profiles.

Tick the box of untrust interface to enable this interface for IPSec access. Press the button "**Add**" to increase a connection profile.



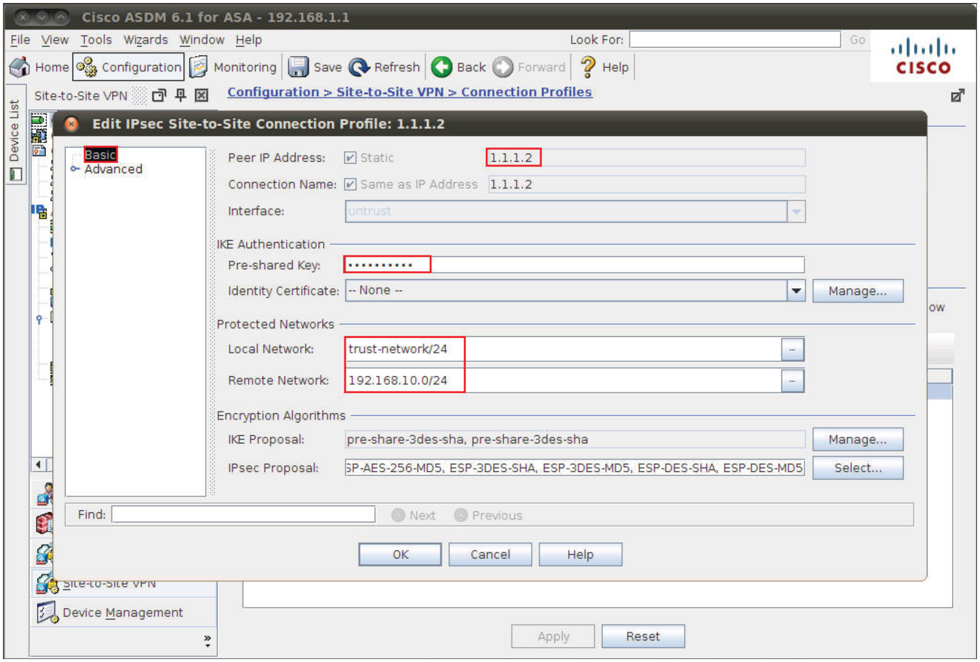
Enable interfaces for IPsec access.

Interface	Allow Access
trust	□
untrust	☑

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters.

Name	Interface	Local Network	Remote Network	Enabled	Group Policy
1.1.1.2	untrust	trust-network/24	192.168.10.0/24	☑	DfltGrpPolicy

Edit the basic information of this profile with below information. The IP address of **Peer IP Address** refers to the external network connecting point of DSR-1000N which is shown as the point "**c**" on the topology. Insert the **Pre-shared Key** which is as same as the one put in DSR-1000N in the previous step. The internal network group, which is indicates the IP information on **Local Network**, under Cisco 5505 allows access to the **remote network** group, which is indicates the IP information on Remote Network, under DSR-1000N through VPN tunnel.


Cisco ASDM 6.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For: Go
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Device List
Basic
Advanced
Find: Next Previous
OK Cancel Help
Site-to-Site VPN
Device Management
Apply Reset

Configuration > Site-to-Site VPN > Connection Profiles

Edit IPsec Site-to-Site Connection Profile: 1.1.1.2

Peer IP Address: ☑ Static 1.1.1.2

Connection Name: ☑ Same as IP Address 1.1.1.2

Interface: untrust

IKE Authentication

Pre-shared Key: ••••••••••

Identity Certificate: -- None -- Manage...

Protected Networks

Local Network: trust-network/24

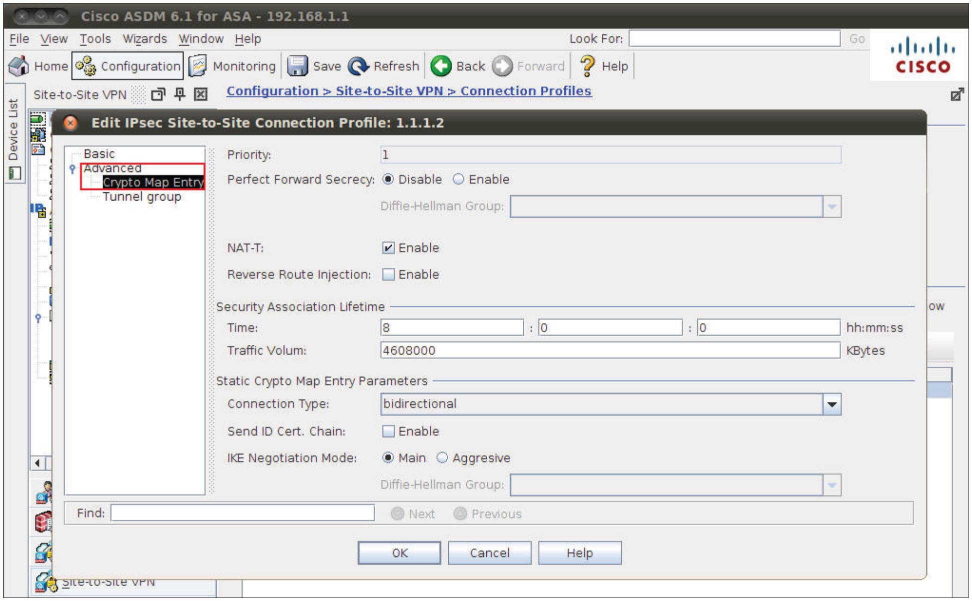
Remote Network: 192.168.10.0/24

Encryption Algorithms

IKE Proposal: pre-share-3des-sha, pre-share-3des-sha Manage...

IPsec Proposal: SP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5 Select...

Click "**Advanced**" in the menu on the left side of the screen. Click "**Crypto Map Entry**" and edit relative information as below.


Cisco ASDM 6.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For: Go
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Device List
Basic
Advanced
Crypto Map Entry
Tunnel group
Find: Next Previous
OK Cancel Help
Site-to-Site VPN

Configuration > Site-to-Site VPN > Connection Profiles

Edit IPsec Site-to-Site Connection Profile: 1.1.1.2

Priority: 1

Perfect Forward Secrecy: ● Disable ○ Enable

Diffie-Hellman Group:

NAT-T: ☑ Enable

Reverse Route Injection: □ Enable

Security Association Lifetime

Time: 8 : 0 : 0 hh:mm:ss

Traffic Volum: 4608000 KBytes

Static Crypto Map Entry Parameters

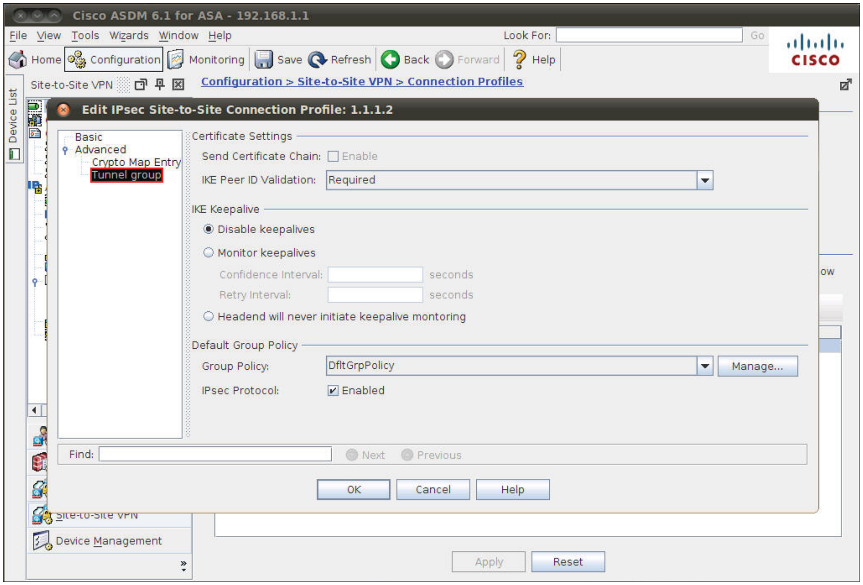
Connection Type: bidirectional

Send ID Cert. Chain: □ Enable

IKE Negotiation Mode: ● Main ○ Aggresive

Diffie-Hellman Group:

Click "**Tunnel group**" and edit relative information as below.


Cisco ASDM 6.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For: Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Site-to-Site VPN
Configuration > Site-to-Site VPN > Connection Profiles
Device List
Basic
Advanced
Crypto Map Entry
Tunnel group
Find: Next Previous
OK Cancel Help
Site-to-Site VPN
Device Management
Apply Reset

Edit IPsec Site-to-Site Connection Profile: 1.1.1.2

Certificate Settings

Send Certificate Chain: □ Enable

IKE Peer ID Validation: Required

IKE Keepalive

● Disable keepalives

○ Monitor keepalives

Confidence Interval: seconds

Retry Interval: seconds

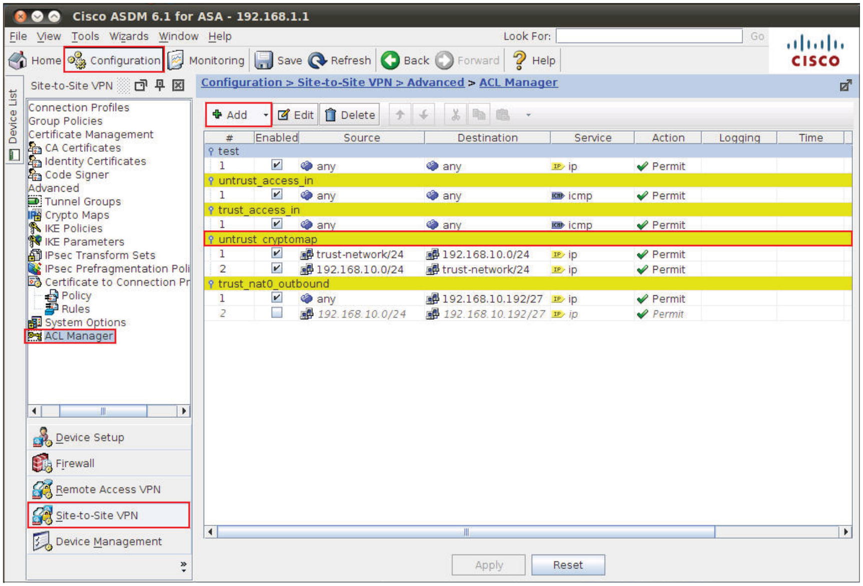
○ Headend will never initiate keepalive montoring

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

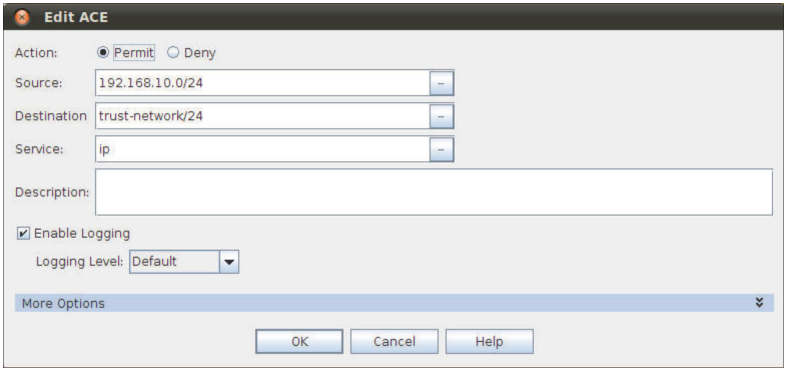
IPsec Protocol: ☑ Enabled

4. Set up the ACL. Navigate to Configuration > Site-to-Site VPN > ACL Manager. Select the **untrust_cyrptomap** and then click the button "**Add**".



Configuration > Site-to-Site VPN > Advanced > ACL Manager

#	Enabled	Source	Destination	Service	Action	Logging	Time
test							
1	☑	any	any	ip	✓ Permit		
untrust_access_in							
1	☑	any	any	icmp	✓ Permit		
trust_access_in							
1	☑	any	any	icmp	✓ Permit		
untrust_cryptomap							
1	☑	trust-network/24	192.168.10.0/24	ip	✓ Permit		
2	☑	192.168.10.0/24	trust-network/24	ip	✓ Permit		
trust_nat0_outbound							
1	☑	any	192.168.10.192/27	ip	✓ Permit		
2	□	192.168.10.0/24	192.168.10.192/27	ip	✓ Permit		



Edit ACE

Action: ● Permit ○ Deny

Source: 192.168.10.0/24

Destination: trust-network/24

Service: ip

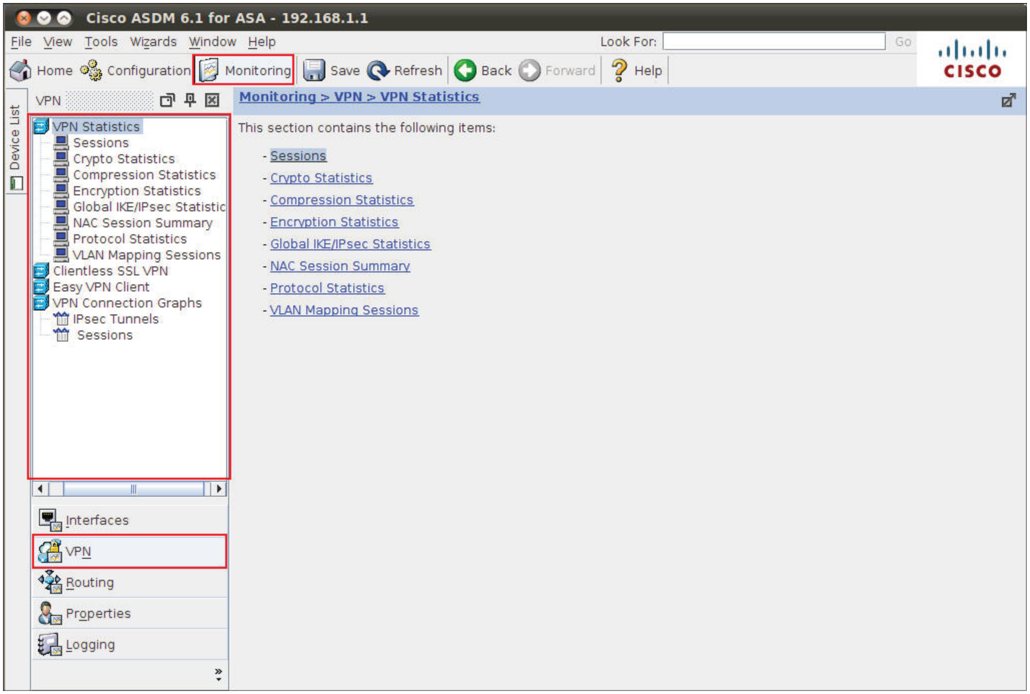
Description:

☑ Enable Logging

Logging Level: Default

More Options

5. Check the VPN status. Navigate to Monitoring > VPN. Select information you want to check from the list.



Cisco ASDM 6.1 for ASA - 192.168.1.1

Monitoring > VPN > VPN Statistics

This section contains the following items:

- Sessions
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/IPsec Statistics
- NAC Session Summary
- Protocol Statistics
- VLAN Mapping Sessions

D-Link®

Visit our website for more information
www.dlink.com