Configuration Guide

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

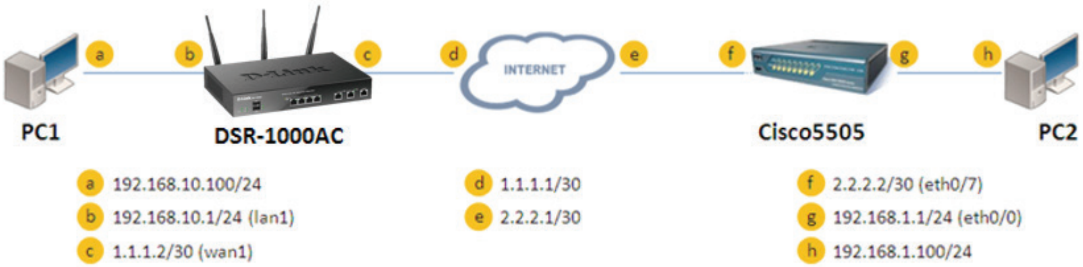
Overview

This document describes how to implement IPsec with pre-shared secrets establishing a site-to-site VPN tunnel between the D-Link DSR-1000AC and the Cisco ASA5505. The screenshots in this document are from firmware version 3.10 of the DSR-1000AC and firmware version 8.0(4) of the Cisco ASA5505. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see in your browser.

D-Link®

Situation note

Site-to-site VPNs can be implemented in an enterprise to allow access and the exchange of data between two or more geographically separated sites or offices. Once the site-to-site VPN has been set up, the clients in the groups of the different sites can communicate as if they are on the same internal network. Because companies may have other gateways that are not D-Link products, this document can be used to create IPsec tunnels between the DSR router and other existing gateway appliances.



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:

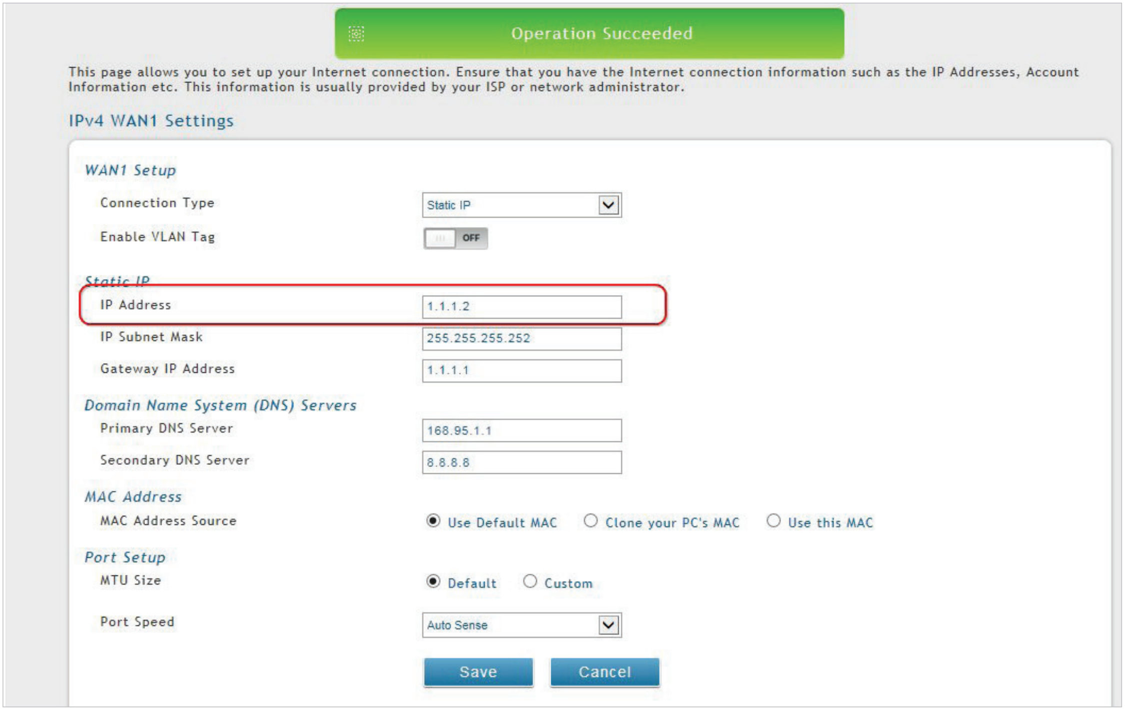
IPsec Mode: **Tunnel Mode**
IPsec Protocol: **ESP**
Phase1 Exchange Mode: **Main**
Phase1 Encryption: **3DES**
Phase1 Authentication: **SHA1**
Phase1 Authentication Method: **Pre-Shared Key**

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: Internet Settings > WAN1 Settings > WAN1 Setup.
Fill in the relevant information based on the settings of the topology. The **IP Address** of the ISP Connection Type field is the IP address of the external network connection shown as point "**c**" in the topology. Click the "**Save**" button to complete the WAN IP address setting.



Operation Succeeded

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.

IPv4 WAN1 Settings

WAN1 Setup

Connection Type	Static IP
Enable VLAN Tag	OFF

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

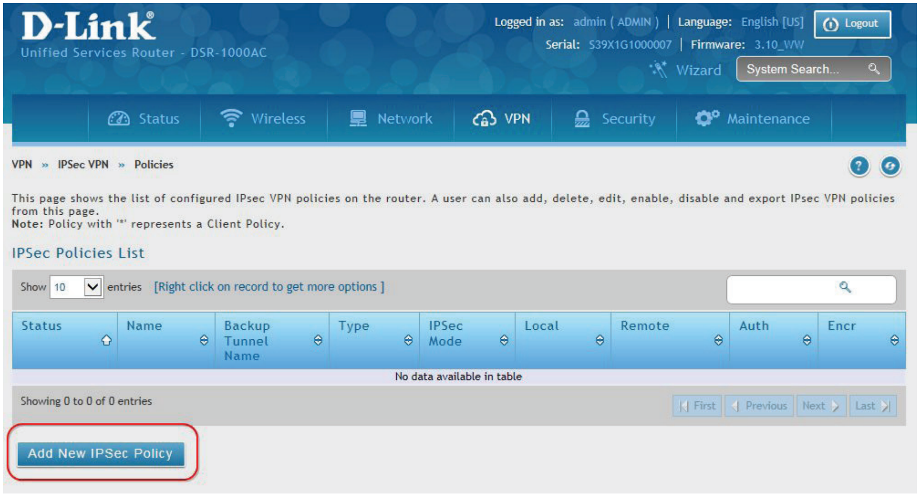
MAC Address Source	● Use Default MAC ○ Clone your PC's MAC ○ Use this MAC

Port Setup

MTU Size	● Default ○ Custom
Port Speed	Auto Sense

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

Press the button "**Add New IPsec Policy**" to create a new policy. In the General section, fill in the relevant information. The IP address of the **Remote Endpoint** refers to the external connection of the Cisco ASA5505, which is shown as the point "**f**" in the topology. The internal IP address range, which is indicated by the **Local Start IP Address**, is the IP range allowed access to the remote network over the VPN, and the remote network range, indicated by the **Remote Start IP Address**, is the IP range reachable through the VPN tunnel with the Cisco ASA5505.



Logged in as: admin (ADMIN) | Language: English [US]

Serial: S39X1G1000007 | Firmware: 3.10_WW

VPN » IPSec VPN » Policies

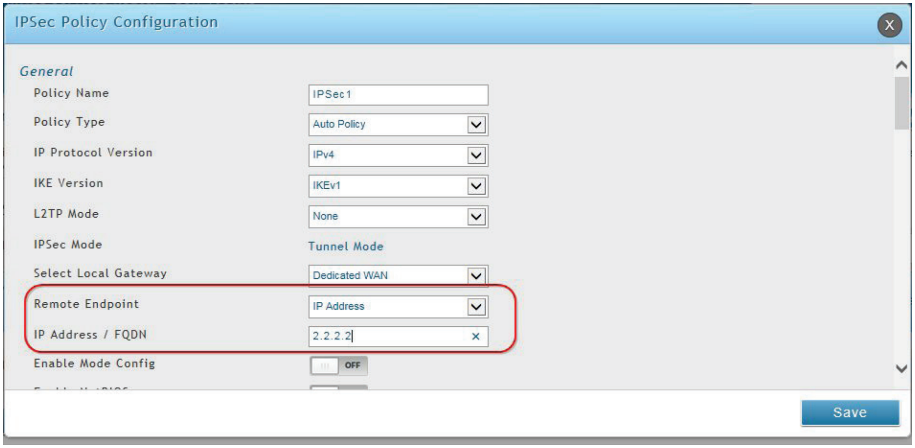
This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with '*' represents a Client Policy.

IPSec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
No data available in table								

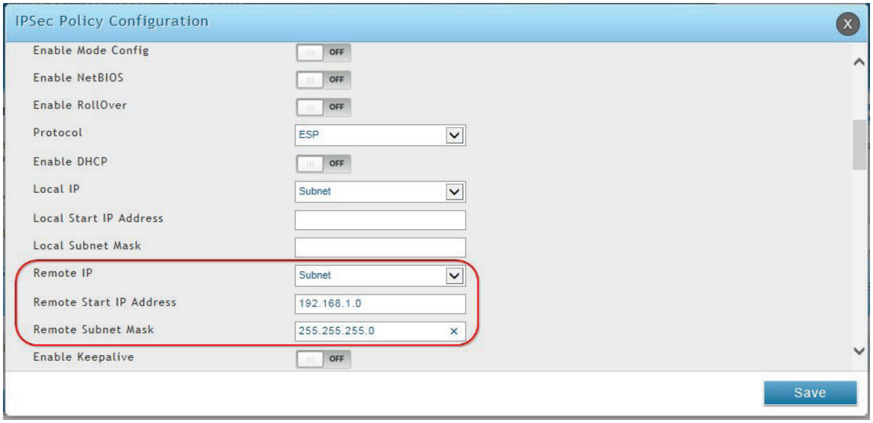
Showing 0 to 0 of 0 entries



IPSec Policy Configuration

General

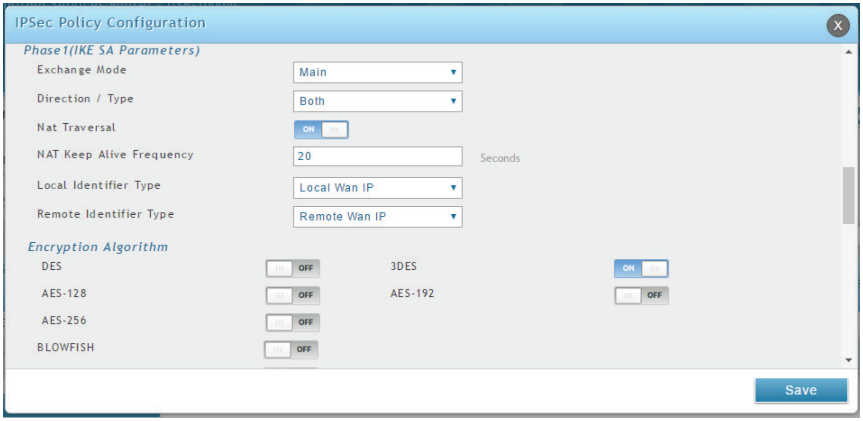
Policy Name	IPSec1
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local Gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address / FQDN	2.2.2.2
Enable Mode Config	OFF



IPSec Policy Configuration

Enable Mode Config	OFF
Enable NetBIOS	OFF
Enable RollOver	OFF
Protocol	ESP
Enable DHCP	OFF
Local IP	Subnet
Local Start IP Address	
Local Subnet Mask	
Remote IP	Subnet
Remote Start IP Address	192.168.1.0
Remote Subnet Mask	255.255.255.0
Enable Keepalive	OFF

In the Phase 1 section, fill in the relevant information. Please notice that the **Pre-shared Key** must be the same as the pre-shared key that will be entered into the Cisco ASA5505 later.



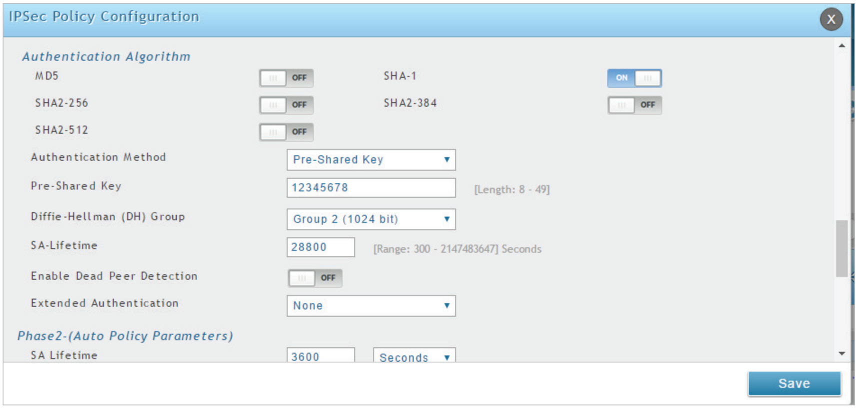
IPSec Policy Configuration

Phase 1(IKE SA Parameters)

Exchange Mode	Main
Direction / Type	Both
Nat Traversal	ON
NAT Keep Alive Frequency	20 Seconds
Local Identifier Type	Local Wan IP
Remote Identifier Type	Remote Wan IP

Encryption Algorithm

DES	OFF	3DES	ON
AES-128	OFF	AES-192	OFF
AES-256	OFF		
BLOWFISH	OFF		



IPSec Policy Configuration

Authentication Algorithm

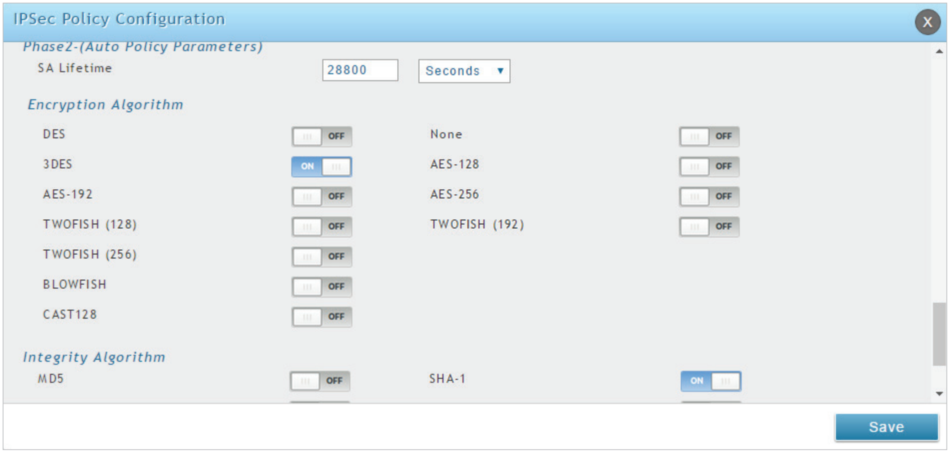
MD5	OFF	SHA-1	ON
SHA2-256	OFF	SHA2-384	OFF
SHA2-512	OFF		

Authentication Method	Pre-Shared Key
Pre-Shared Key	12345678 [Length: 8 - 49]
Diffie-Hellman (DH) Group	Group 2 (1024 bit)
SA-Lifetime	28800 [Range: 300 - 2147483647] Seconds
Enable Dead Peer Detection	OFF
Extended Authentication	None

Phase2-(Auto Policy Parameters)

SA Lifetime	3600 Seconds

In the Phase 2 section, fill in the relevant information.



IPSec Policy Configuration

Phase2-(Auto Policy Parameters)

SA Lifetime 28800 Seconds

Encryption Algorithm

DES	OFF	None	OFF
3DES	ON	AES-128	OFF
AES-192	OFF	AES-256	OFF
TWOFISH (128)	OFF	TWOFISH (192)	OFF
TWOFISH (256)	OFF		
BLOWFISH	OFF		
CAST128	OFF		

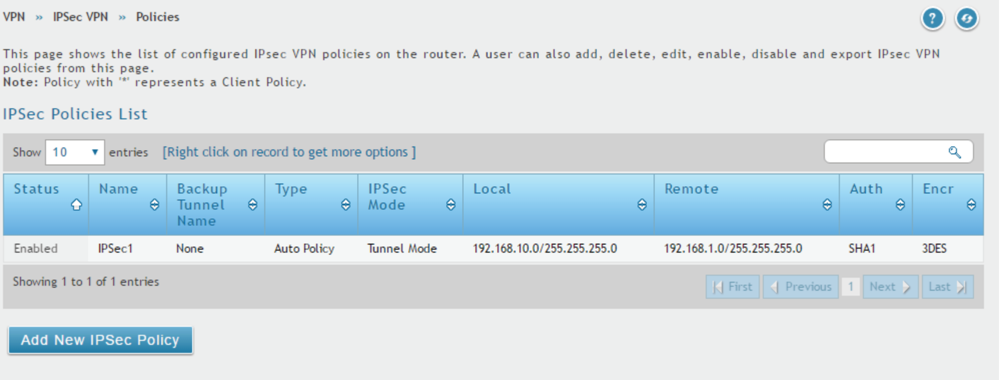
Integrity Algorithm

MD5	OFF	SHA-1	ON

Click the "**Save**" button to complete the IPsec Policy settings.

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

The activity will be shown in the list as the tunnel is established with the other side.



VPN » IPSec VPN » Policies

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with '*' represents a Client Policy.

IPSec Policies List

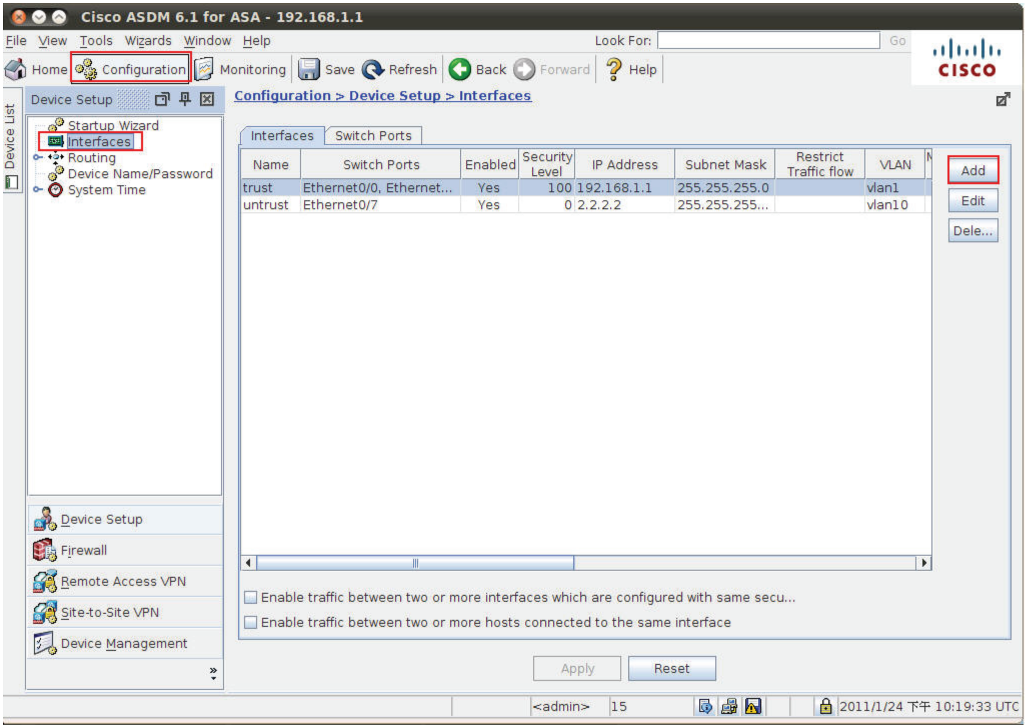
Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	IPSec1	None	Auto Policy	Tunnel Mode	192.168.10.0/255.255.255.0	192.168.1.0/255.255.255.0	SHA1	3DES

Showing 1 to 1 of 1 entries

Cisco ASA5505 Settings

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

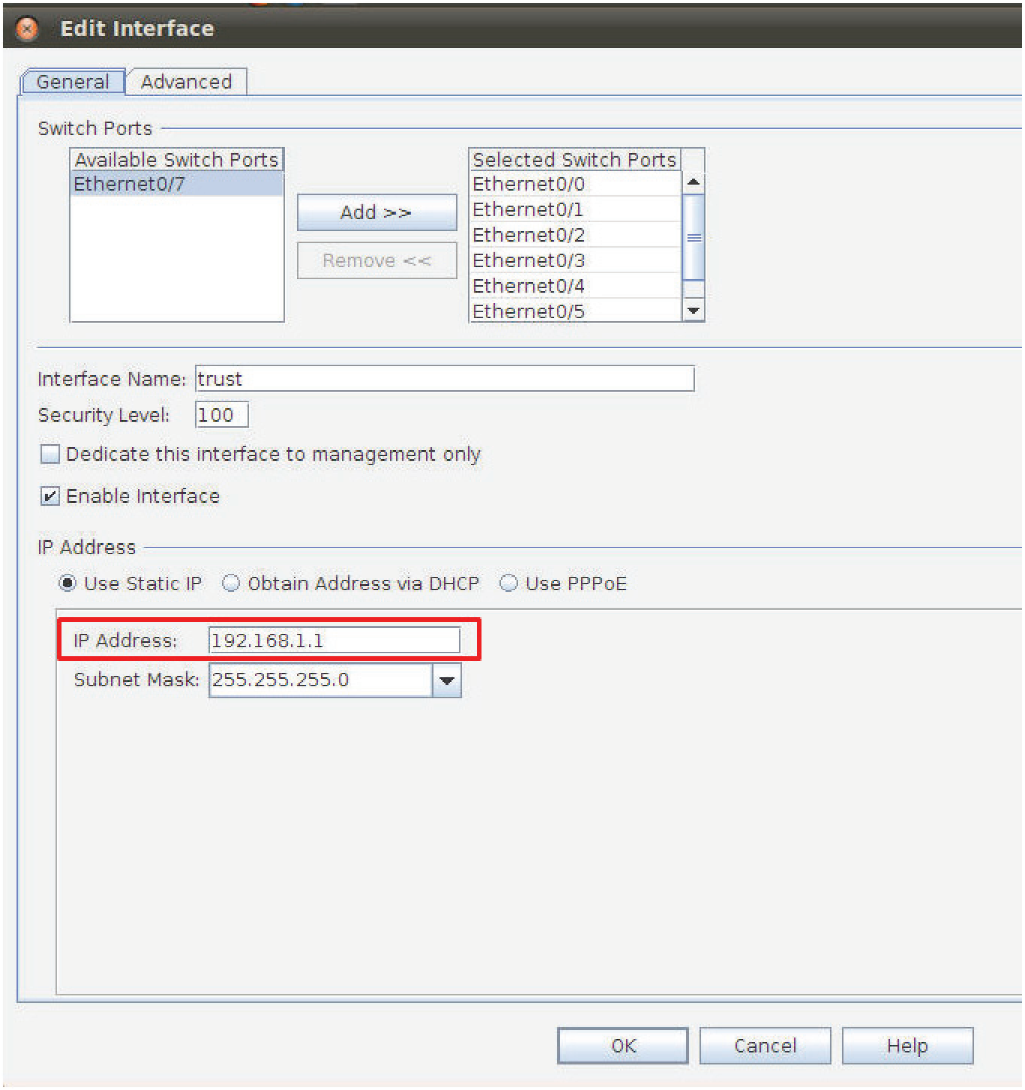


Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask	Restrict Traffic flow	VLAN	M
trust	Ethernet0/0, Ethernet...	Yes	100	192.168.1.1	255.255.255.0		vlan1	
untrust	Ethernet0/7	Yes	0	2.2.2.2	255.255.255...		vlan10	

□ Enable traffic between two or more interfaces which are configured with same secu...

□ Enable traffic between two or more hosts connected to the same interface

First, edit the trusted interface. Select and fill in the relevant information as below. The **IP Address** of the General tab is the IP address of internal network connection, which is shown as point "g" in the topology. Click the "**OK**" button to finish the configuration.



Edit Interface

General | Advanced

Switch Ports

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

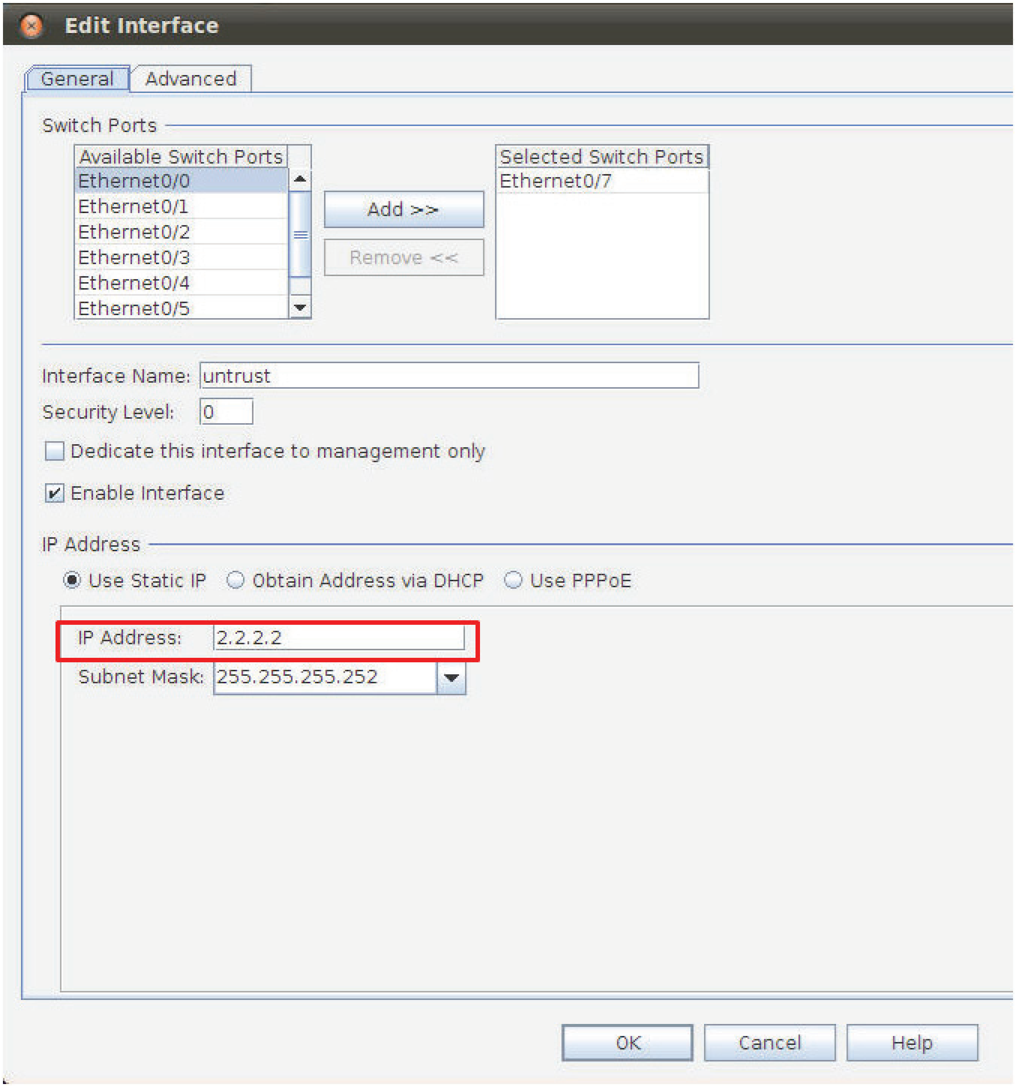
IP Address

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Second, edit the untrusted interface. Select and fill in relevant information as below. The **IP Address** of General tab is the IP address of external network connection, which is shown as point "**f**" on the topology. Click the button "**OK**" to finish the configuration.



Edit Interface

General | Advanced

Switch Ports

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

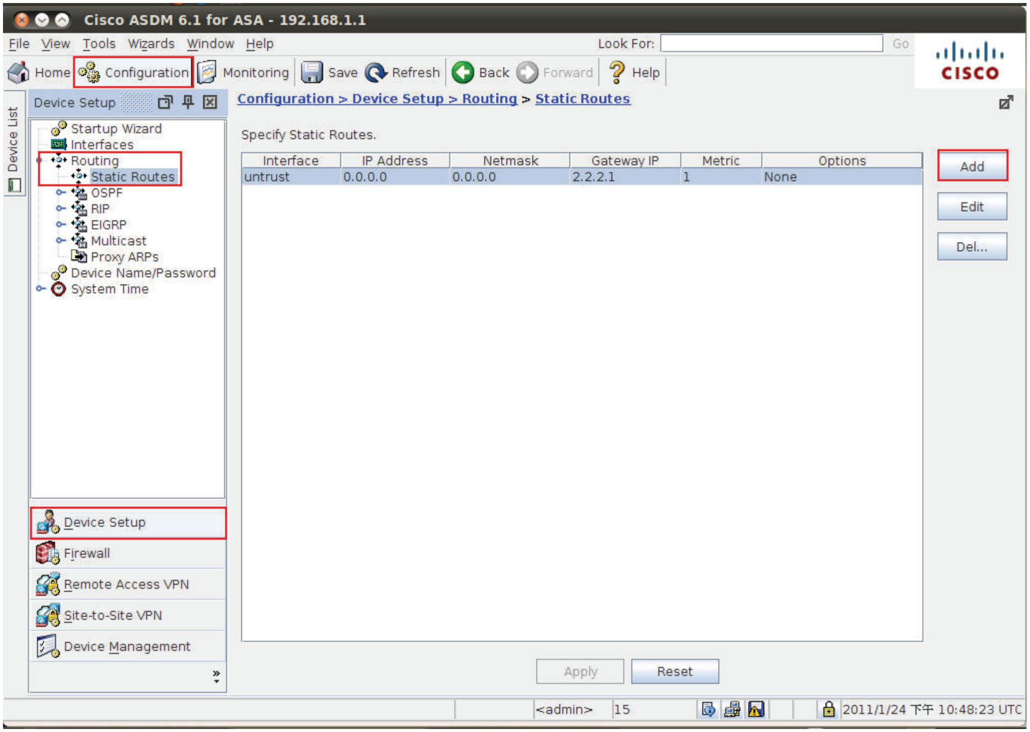
● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

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 "**Add**" button.

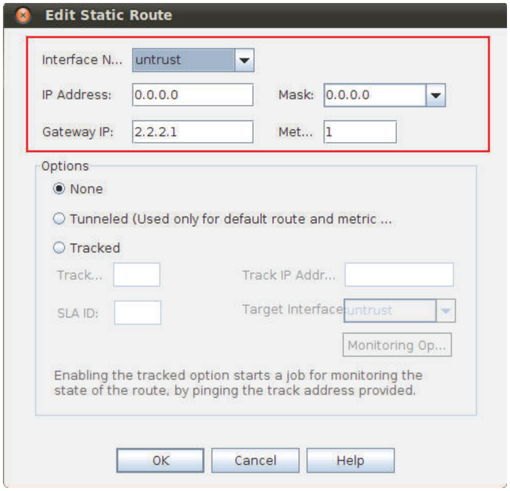


Configuration > Device Setup > Routing > Static Routes

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 the untrusted interface as the default gateway interface. Fill in relevant 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

Options

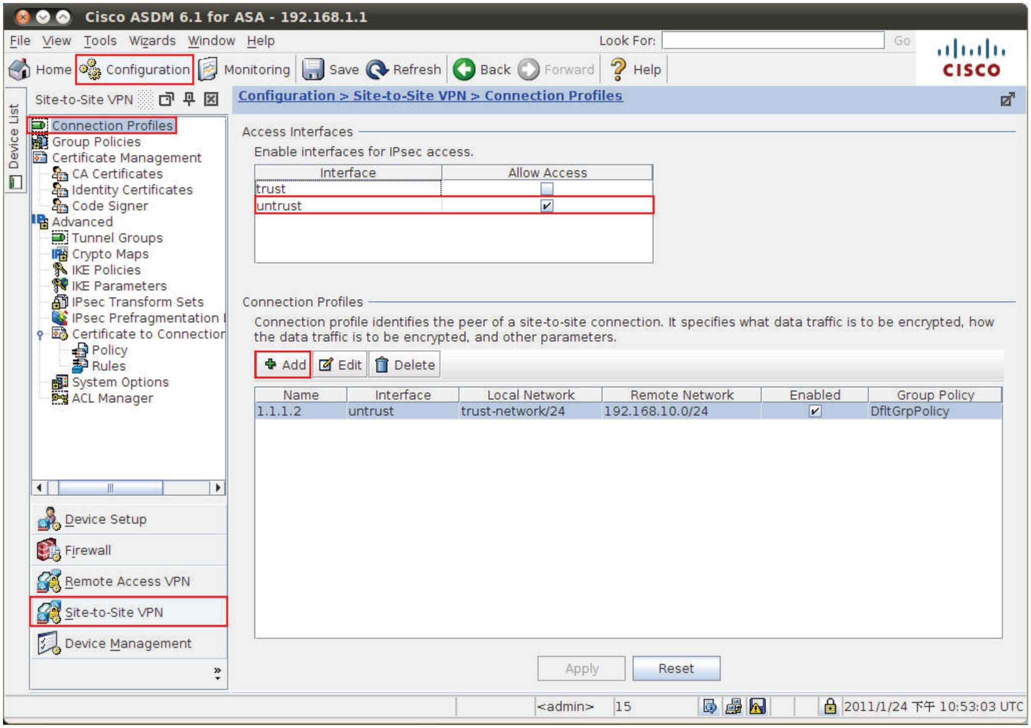
● None

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

○ Tracked

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: Configuration > Site-to-Site VPN > Connection Profiles.
Tick the box of the untrusted interface to enable this interface for IPsec access. Press the "**Add**" button to create a connection profile.



Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
trust	☐
untrust	☑

Connection Profiles

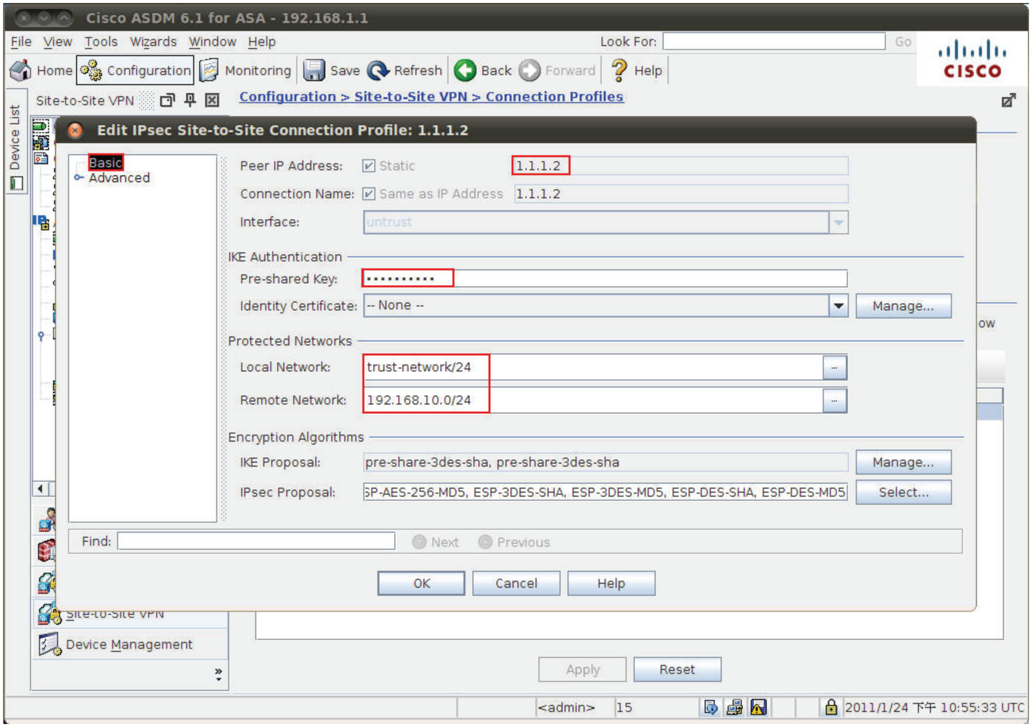
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters.

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 connection of the DSR-1000AC, which is shown as point "**c**" on the topology. Enter the **Pre-shared Key** which was entered in the DSR-1000AC earlier.

The internal IP address range, indicated by the **Local Network** field, is the range of addresses allowed access to the remote network over the VPN, and the remote network range, indicated by the **Remote Network** field, is the IP address range reachable through the VPN with the DSR-1000AC.


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
Configuration > Site-to-Site VPN > Connection Profiles
Device List
Site-to-Site VPN
Device Management
Apply Reset
<admin> 15 2011/1/24 下午 10:55:33 UTC

Edit IPsec Site-to-Site Connection Profile: 1.1.1.2

Basic
Advanced

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...

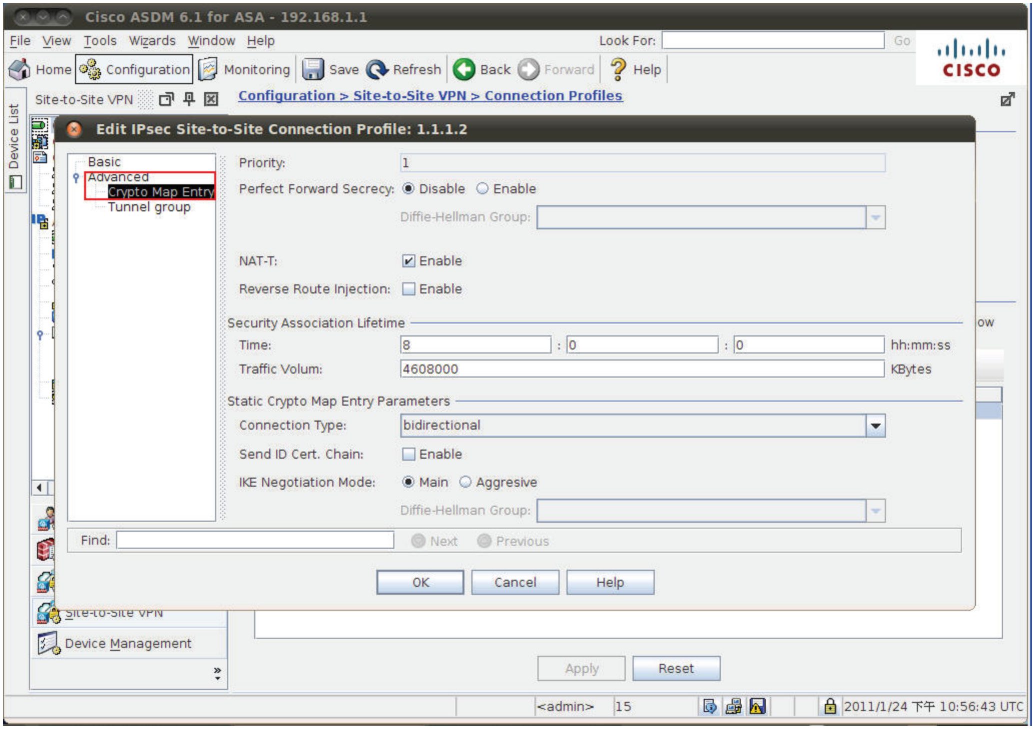
Protected Networks
Local Network: trust-network/24
Remote Network: 192.168.10.0/24

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...

Find: ○ Next ○ Previous

OK Cancel Help

Click "**Advanced**" in the menu on the left side of the screen. Click "Crypto Map Entry" and edit the relevant 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
Device List
Configuration > Site-to-Site VPN > Connection Profiles
Edit IPsec Site-to-Site Connection Profile: 1.1.1.2
Basic
Advanced
Crypto Map Entry
Tunnel group
Find: Next Previous
OK Cancel Help
Site-to-Site VPN
Device Management
Apply Reset
<admin> 15
2011/1/24 下午 10:56:43 UTC

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

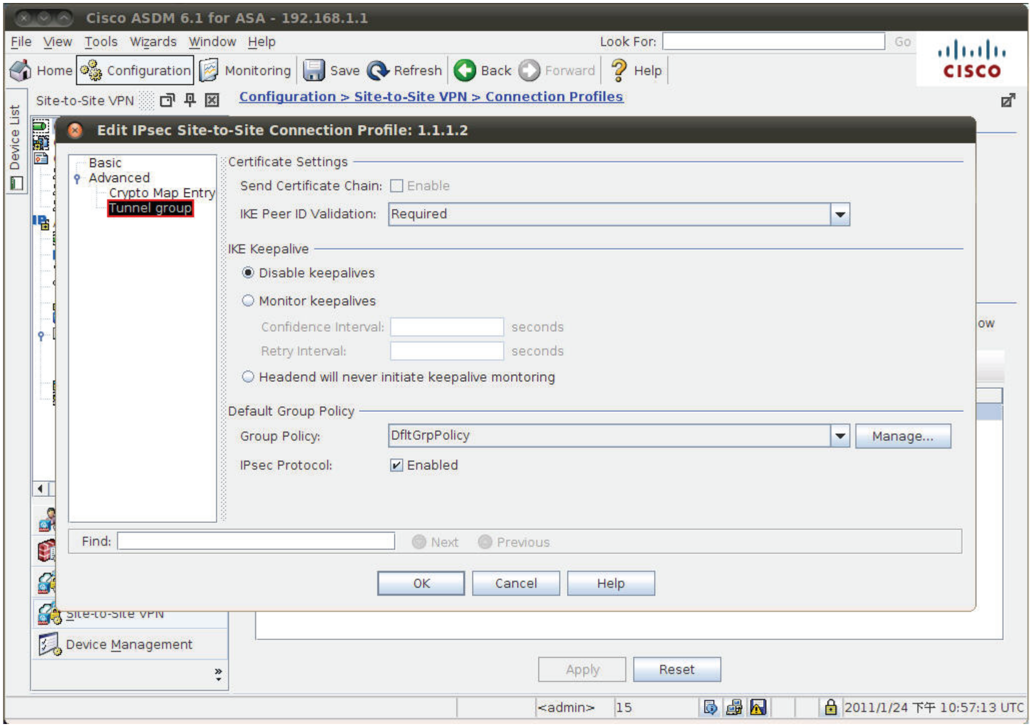
Connection Type: bidirectional

Send ID Cert. Chain: □ Enable

IKE Negotiation Mode: ● Main ○ Aggresive

Diffie-Hellman Group:

Click “**Tunnel group**” and edit relevant information as below.



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

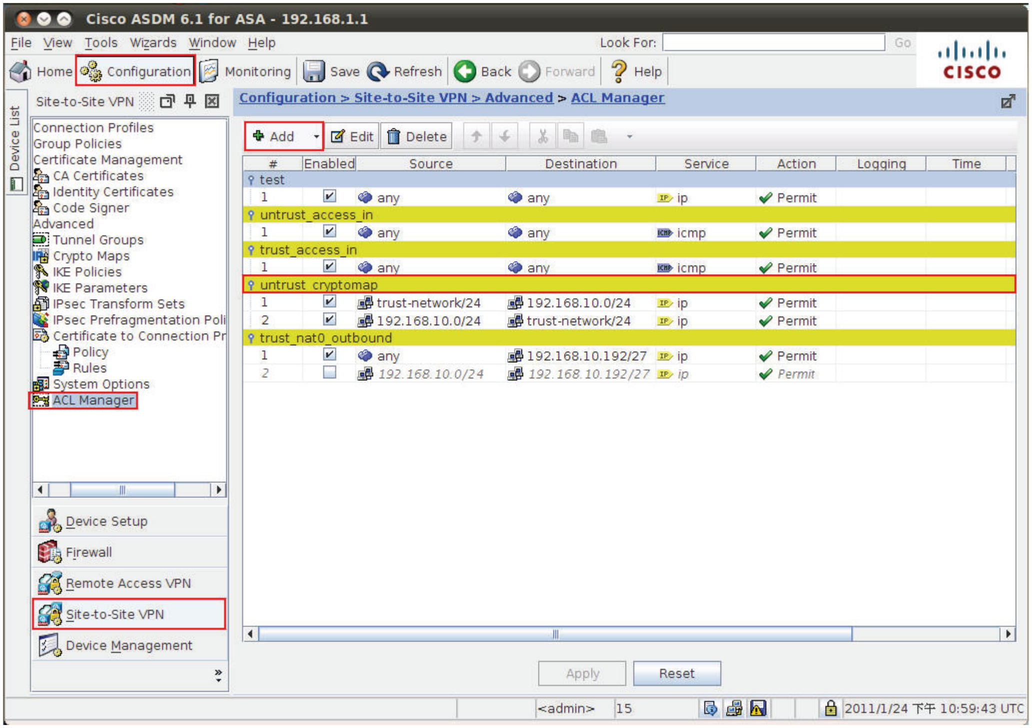
Group Policy: DfltGrpPolicy

IPsec Protocol: ☑ Enabled

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
Configuration > Site-to-Site VPN > Connection Profiles
Device List
Basic
Advanced
Crypto Map Entry
Tunnel group
Manage...
Find: Next Previous
OK Cancel Help
Site-to-Site VPN
Device Management
Apply Reset
<admin> 15
2011/1/24 下午 10:57:13 UTC

4. Set up the ACL. Navigate to: Configuration > Site-to-Site VPN > ACL Manager.

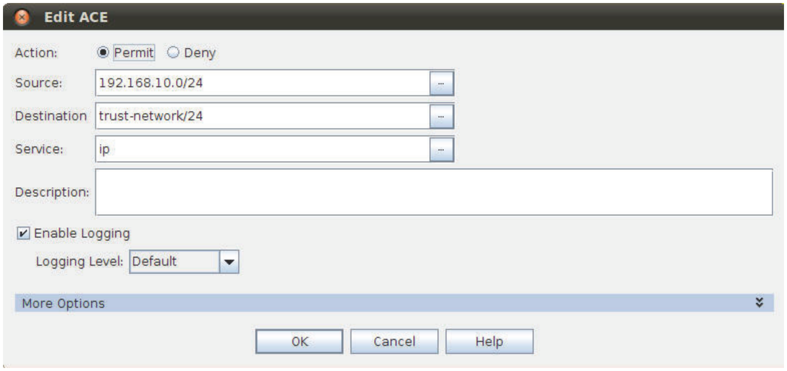
Select the **untrust_cyrptomap** and then click the "**Add**" button.



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 with below information.



Action: ● Permit ○ Deny

Source: 192.168.10.0/24

Destination trust-network/24

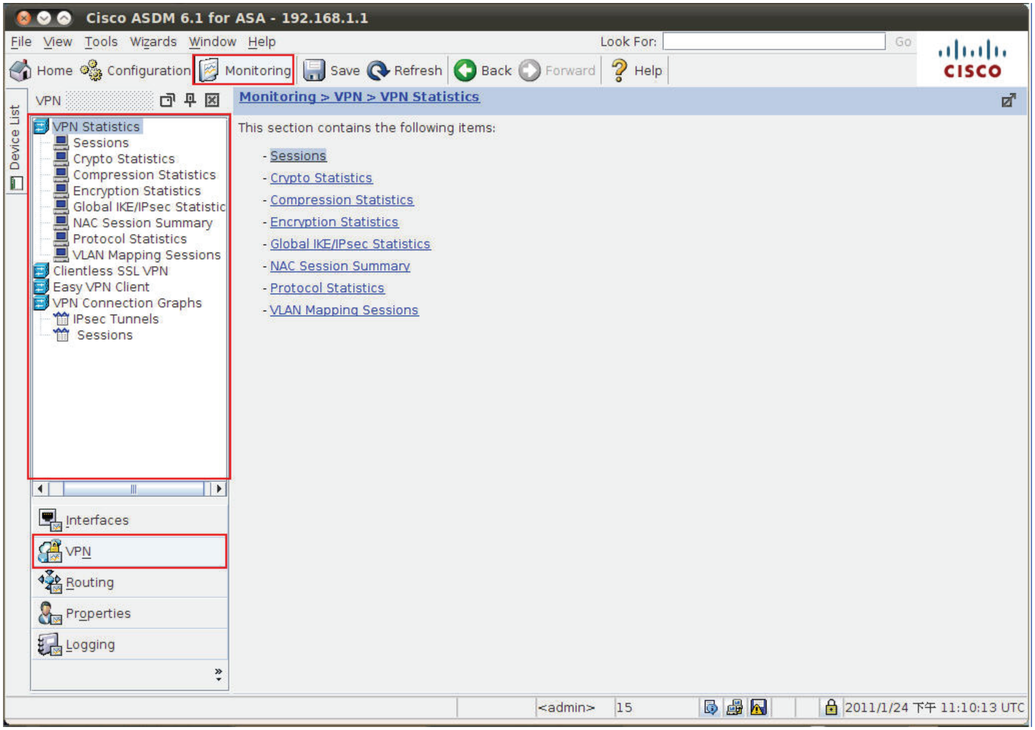
Service: ip

Description:

☑ Enable Logging

Logging Level: Default

5. Check the VPN status. Navigate to: Monitoring > VPN.
Select the entries that you wish to view from the list.



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