



Site-to-Site IPSec Interoperability between ATERA Networks CL-Series Security Router and Cisco 2651XM

Table of Contents

Table of Contents	1
Introduction	2
Components Used	2
Network Setup.....	2
Configuration Example	3
Citadel CL-100 Configuration	3
Cisco 2651XM Router Configuration.....	4

Introduction

IPSec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity, and authenticity of data communications across a public network. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network wide security policy.

Citadel CL-Series Security Routers supports IPSec site-to-site connectivity and is interoperable with other IPSec-enabled security devices such as Cisco Routers, Cisco PIX, Checkpoint Firewalls etc. Following is a configuration example for site-to-site IPSec VPN between a Citadel CL-100 Security Router and a Cisco 2651XM router.

Components Used

In this setup we used the following components:

- ATERA Networks CL-100 VPN Router, running firmware version 2.20 Build 0132.
- 2651XM Router, running IOS (tm) C2600 Software (C2600-JK9S-M), Version 12.2(26), RELEASE SOFTWARE (fc2)

Network Setup

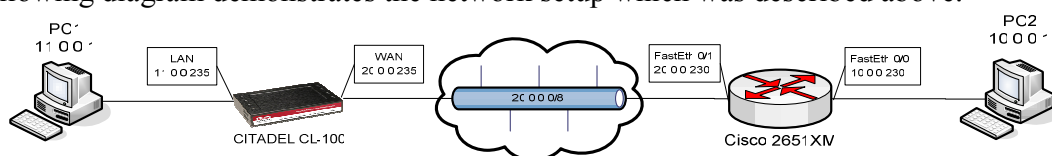
In order to simulate IPSec VPN connectivity between two remote LANs, we created the following setup:

PC1 was connected to the LAN interface of the Citadel CL-100 Router. PC1 was configured with IP address of 11.0.0.1/8. The CL-100 LAN interface was configured with IP address of 11.0.0.235/8, and was acting as the default gateway for PC1.

PC2 was connected to FastEthernet0/0 interface of a Cisco 2651XM router. PC2 was configured with IP address of 10.0.0.1/8. The Cisco router FastEthernet0/0 interface was configured with IP address of 10.0.0.230/8, and was acting as the default gateway for PC2.

Both CL-100's WAN interface and Cisco's FastEthernet0/1 interface were connected to a Fast Ethernet switch. CL-100's WAN IP address was configured as 20.0.0.235/8. Cisco's interface was configured as 20.0.0.230/8.

The following diagram demonstrates the network setup which was described above:



Configuration Example

Citadel CL-100 Configuration

By default, Citadel CL-Series router negotiates four proposals of IPSec:

- 3DES, MD5, DH Group2
- 3DES, SHA-1, DH Group2
- 3DES, MD5, DH Group 5
- 3DES, SHA-1, DH Group 5

IPSec VPN

Enable IPSec VPN :

IPSEC MTU : [0~1440]

Tunnel Name :

Local Network IP Address :

Local Network Subnet Mask :

Remote Node ID (Optional) :

Remote Node IP Address/Hostname :

Remote Network Address :

Remote Network Subnet Mask :

Using PFS :

Authentication :

IPSec Lifetime (seconds) :

IKE Lifetime (seconds) :

Enabled :

Select	Tunnel Name	Local Network	Remote Node	Remote Network	Using PFS	IPSec Lifetime (seconds)	IKE Lifetime (seconds)	Enabled/ Disabled	Status
<input checked="" type="radio"/>	test	11.0.0.0/8	20.0.0.230	10.0.0.0/8	Yes	3600	3600	Enabled	UP

Cisco 2651XM Router Configuration

We configured the Cisco router to negotiate the following parameters: 3DES, MD5, DH Group 5, in order to encrypt all traffic between 10.0.0.0/8 network and 11.0.0.0/8 network.

Router#sh run

Building configuration...

Current configuration : 1064 bytes

```
!  
version 12.2  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname Router  
!  
logging buffered 4096 debugging  
enable secret 5 xxxxxxxxxxxx  
!  
ip subnet-zero  
!  
ip name-server 10.0.0.2  
!
```

!-- Internet Key Exchange (IKE) configuration.

```
crypto isakmp policy 1  
  encr 3des  
  hash md5  
  authentication pre-share  
  group 5
```

!-- configuring the pre-shared key

```
crypto isakmp key 0123456789012345 address 20.0.0.235 255.0.0.0  
!
```

!-- IPSec configuration

*!-- the transform which is used against the Citadel – 3DES Encryption of the ESP payload, MD5
!-- as hashing algorithm. These settings are also supported by the Citadel router.*

```
crypto ipsec transform-set myset esp-3des esp-md5-hmac  
!  
crypto map mymap 5 ipsec-isakmp
```

```
set peer 20.0.0.235
set transform-set myset
match address 100
```

```
!
call rsvp-sync
!
```

```
interface FastEthernet0/0
ip address 10.0.0.230 255.0.0.0
duplex auto
speed auto
!
```

!-- Enabling IPsec on the interface by applying the crypto map --!

```
interface FastEthernet0/1
ip address 20.0.0.230 255.0.0.0
duplex auto
speed auto
crypto map mymap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 11.0.0.0 255.0.0.0 20.0.0.235
ip http server
!
```

!-- The following access-list defines the network addresses that will be encrypted by the IPsec engine – all traffic from network 10.0.0.0/8 to network 11.0.0.0/8 will be encrypted.

```
access-list 100 permit ip 10.0.0.0 0.0.0.255 11.0.0.0 0.0.0.255
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
password cisco
login
!
end
```