

I got the VPN up between the RV042 and my ASA5505.

I was a bit perplexed during this process, as i kept on getting ISAKMP proposals failing. Then i noticed that my RV042 tunnel was tunnel B .

I discovered that tunnel A on the RV042 would accept any remote tunnel, so i disabled tunnel A on your RV042.

All i did was then was, mirror the settings on the RV042 and my ASA5505 and the tunnel popped open.

I could not ping any other device on the LAN , not sure about the remote Hosts and their setup or firewalls etc..but even the RV042 could not ping any other device on it's own LAN so i assumed that either devices must be turned off or they might have a firewall on these devices that stop ping.

regards Dave

**Figure 1: ping from my PC to your router**

```
Command Prompt
C:\Documents and Settings\dhornste>ping 172.16.10.1 -t
Pinging 172.16.10.1 with 32 bytes of data:
Reply from 172.16.10.1: bytes=32 time=77ms TTL=63
Reply from 172.16.10.1: bytes=32 time=73ms TTL=63
Reply from 172.16.10.1: bytes=32 time=74ms TTL=63
Reply from 172.16.10.1: bytes=32 time=75ms TTL=63
Reply from 172.16.10.1: bytes=32 time=75ms TTL=63
Reply from 172.16.10.1: bytes=32 time=72ms TTL=63
Reply from 172.16.10.1: bytes=32 time=74ms TTL=63
Reply from 172.16.10.1: bytes=32 time=78ms TTL=63
Reply from 172.16.10.1: bytes=32 time=74ms TTL=63
Reply from 172.16.10.1: bytes=32 time=73ms TTL=63
Reply from 172.16.10.1: bytes=32 time=80ms TTL=63
Reply from 172.16.10.1: bytes=32 time=72ms TTL=63
Reply from 172.16.10.1: bytes=32 time=84ms TTL=63
Reply from 172.16.10.1: bytes=32 time=73ms TTL=63
Reply from 172.16.10.1: bytes=32 time=75ms TTL=63
Reply from 172.16.10.1: bytes=32 time=74ms TTL=63
Reply from 172.16.10.1: bytes=32 time=73ms TTL=63
Reply from 172.16.10.1: bytes=32 time=74ms TTL=63
Reply from 172.16.10.1: bytes=32 time=75ms TTL=63
Ping statistics for 172.16.10.1:
    Packets: Sent = 19, Received = 19, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 72ms, Maximum = 84ms, Average = 75ms
Control-C
^C
C:\Documents and Settings\dhornste>
```

Figure 2: Uptime of the tunnel and encryption setup and negotiated parameters

**Session Details** ✖

Session Details

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
65.15.243.167 rv042	IKE IPsec AES128	00:29:17 EDT Wed Mar 18 2009 0h:22m:59s	668203 9435434

Details **ACL**

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx	More
	IKE		AES-128	Tunnel ID: 13.1 Authentication Mode: preSharedKeys UDP Source Port 500 UDP Destination Port 500 IKE Negotiation Mode: Main Hashing: MD5 Diffie-Hellman Group: 2 Rekey Time Interval: 28800 Seconds Rekey Left(T): 27421 Seconds		
	IPsec	192.168.0.0/255.255.0.0/0/0 rv042/255.255.255.0/0/0	AES-128	Tunnel ID: 13.2 Hashing: MD5 Encapsulation: Tunnel PFS Group: 2 Rekey Time Interval: 3600 Seconds Rekey Left(T): 2222 Seconds Idle Time Out: 30 Minutes Idle TO Left: 25 Minutes Packets Tx: 11024 Packets Rx: 19045	668203 9435434	
	NAC			Revalidation Time Interval: 0 Seconds Time Until Next Revalidation: 0 Seconds Status Query Time Interval: 0 Seconds EAPoUDP Session Age: 1379 Seconds Hold-off Time Remaining: 0 Seconds		

Figure 3 : My setup

**Edit IPsec Site-to-Site Connection Profile: 65.15.243.167**

Basic  
Advanced  
Crypto Map Entry  
Tunnel group

Peer IP Address:  Static 65.15.243.167

Connection Name:  Same as IP Address 65.15.243.167

Interface: outside

**IKE Authentication**

Pre-shared Key: ●●●●●●●●

Identity Certificate: -- None --

**Protected Networks**

Local Network: 192.168.0.0/16

Remote Network: 172.16.0.0/16

**Encryption Algorithms**

IKE Proposal: pre-share-aes-md5

IPsec Proposal: ESP-AES-128-MD5

Find:   Next  Previous

Figure 4: My setup

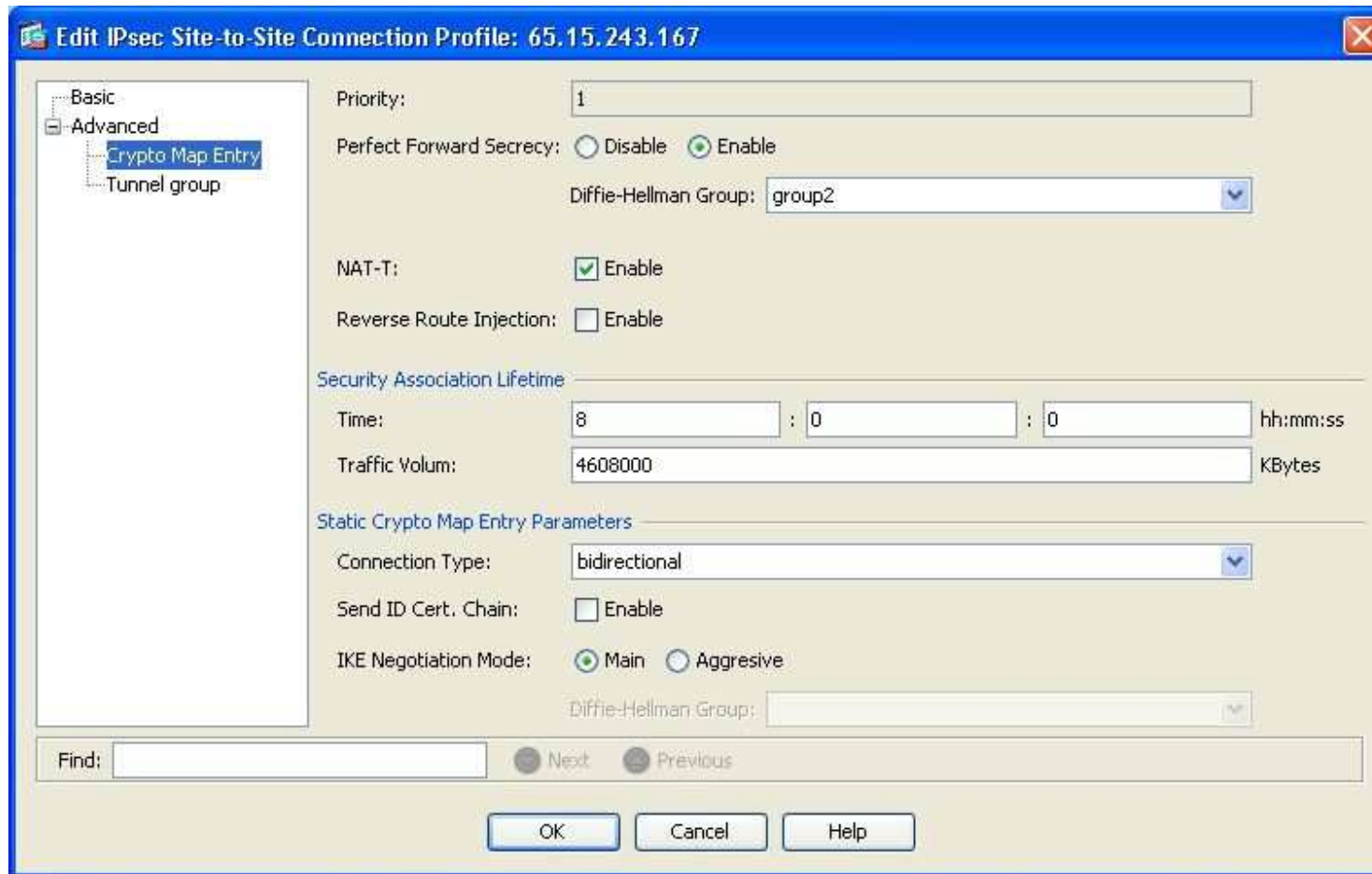


Figure 5: continue of My setup of my ACL in my ASA5505

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

Firewall

- IP Audit Policy
- IP Audit Signat
- SUNRPC Server
- TCP Options
- Global Timeouts
- Virtual Access
- ACL Manager
- Standard ACL

Configuration > Firewall > Advanced > ACL Manager

+ Add Edit Delete [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

#	Enabled	Source	Destination	Service	Action	Logging	Time
inside_access_in							
1	<input checked="" type="checkbox"/>	any	any	IP ip	Permit		
outside_cryptomap							
1	<input checked="" type="checkbox"/>	192.168.0.0/16	172.16.0.0/16	IP ip ICMP icmp	Permit		
outside_access_in							
1	<input checked="" type="checkbox"/>	any	any	ICMP echo-reply	Permit		daily
inside_nat0_outbound							
1	<input checked="" type="checkbox"/>	any	172.16.0.0/16 rv042/24	IP ip	Permit		

Apply Reset

Configuration changes saved successfully. <admin> 15 3/18/09 12:29:...

**Figure 6: Your setup**



**VPN Tunnel**

Tunnel Entry: Tunnel B   
VPN Tunnel:  Enabled  Disabled  
Tunnel Name: Cisco\_Tech  
NAT-Traversal:  Enabled  Disabled

**Local Secure Group**

Type: Subnet   
IP Address: 172 . 16 . 10 . 0  
Mask: 255 . 255 . 255 . 0

**Remote Secure Group**

Type: Subnet   
IP Address: 192 . 168 . 0 . 0  
Mask: 255 . 255 . 0 . 0

**Remote Secure Gateway**

Type: IP Addr.   
IP Address: 24 . 211 . 144 . 46

**Key Management**

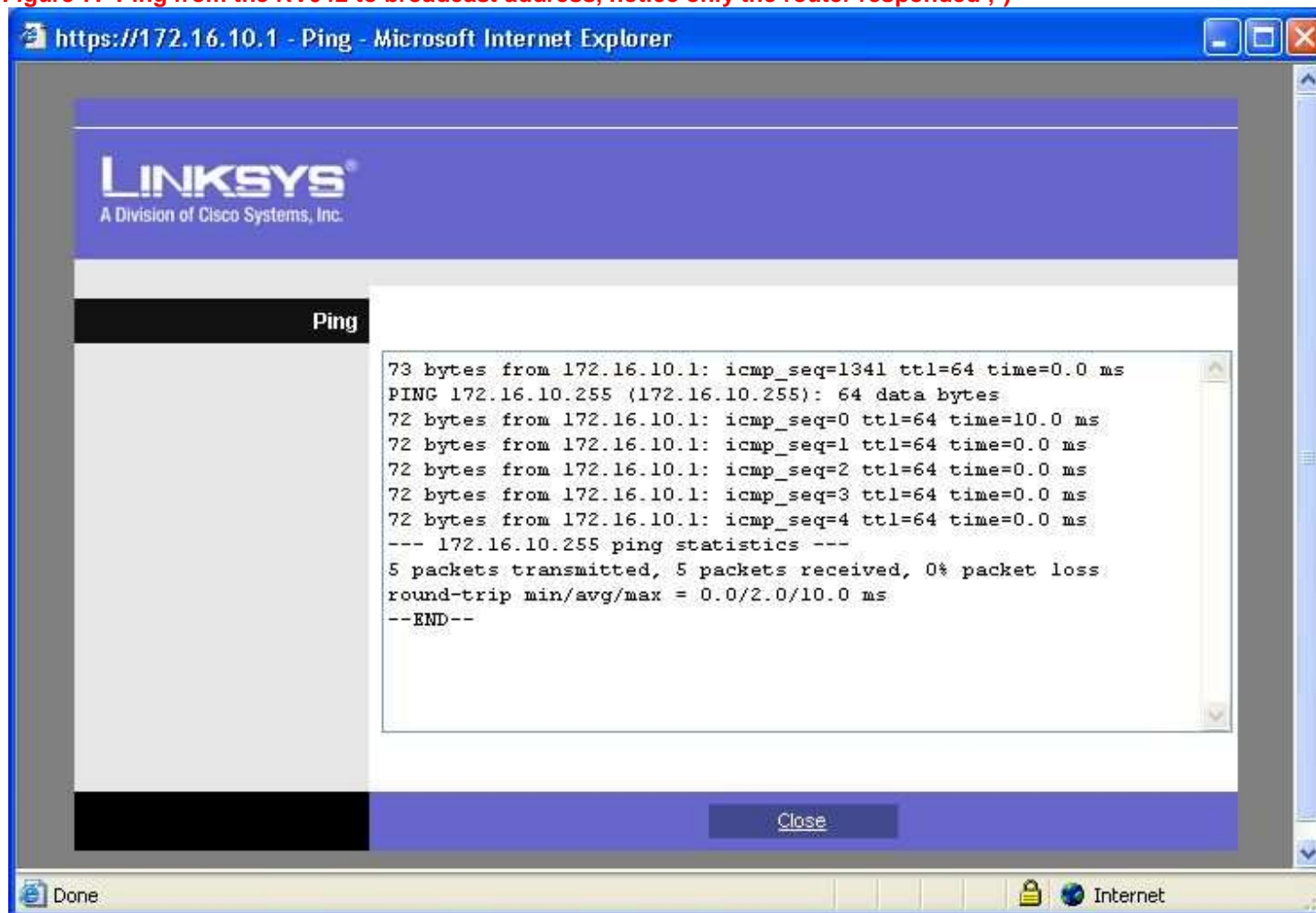
Key Exchange Method: Auto (IKE)   
Operation Mode: Main   
ISAKMP Encryption Method: AES128   
ISAKMP Authentication Method: MD5   
ISAKMP DH Group: Group 2: 1024-bits   
ISAKMP Key Lifetime (s): 28800  
PFS:  Enabled  Disabled  
IPSec Encryption Method: AES128   
IPSec Authentication Method: MD5   
IPSec DH Group: The group is the same as ISAKMP.  
IPSec Key Lifetime(s): 3600  
Pre-Shared Key: 123456789

IPSec VPN  
The VPN Broadband Router creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

[More...](#)



Figure 7: Ping from the RV042 to broadcast address, notice only the router responded ;-)



you owe me a few beers, if it works

regards Dave

---