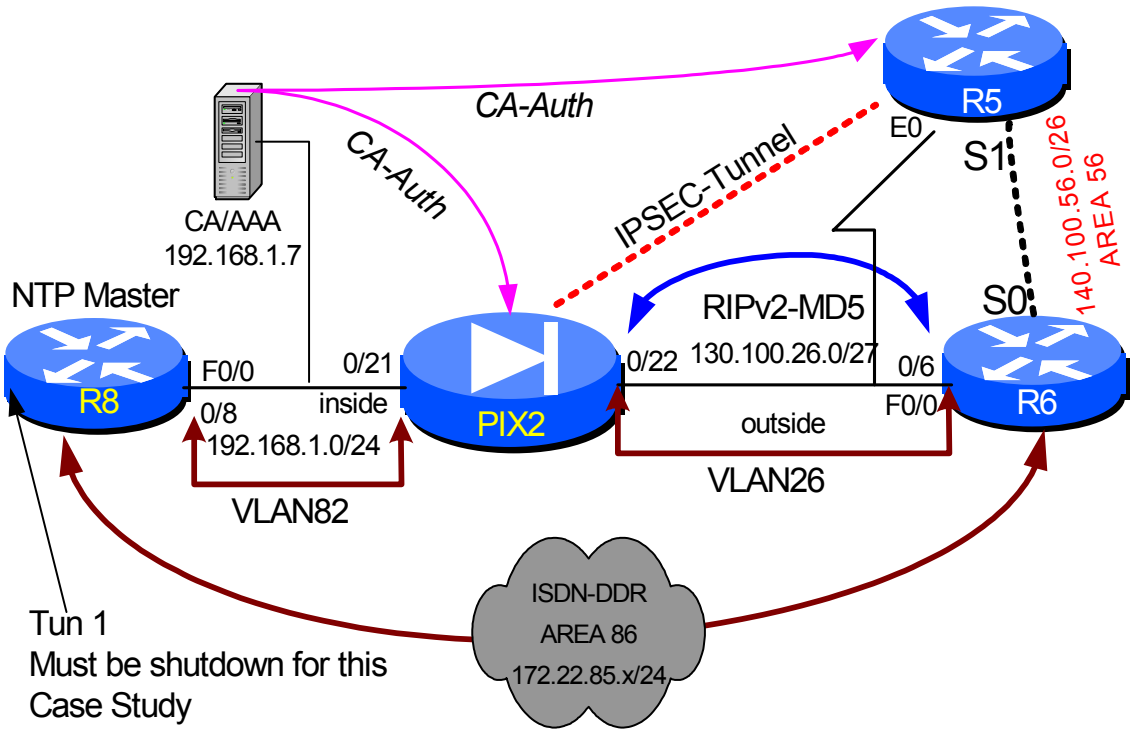
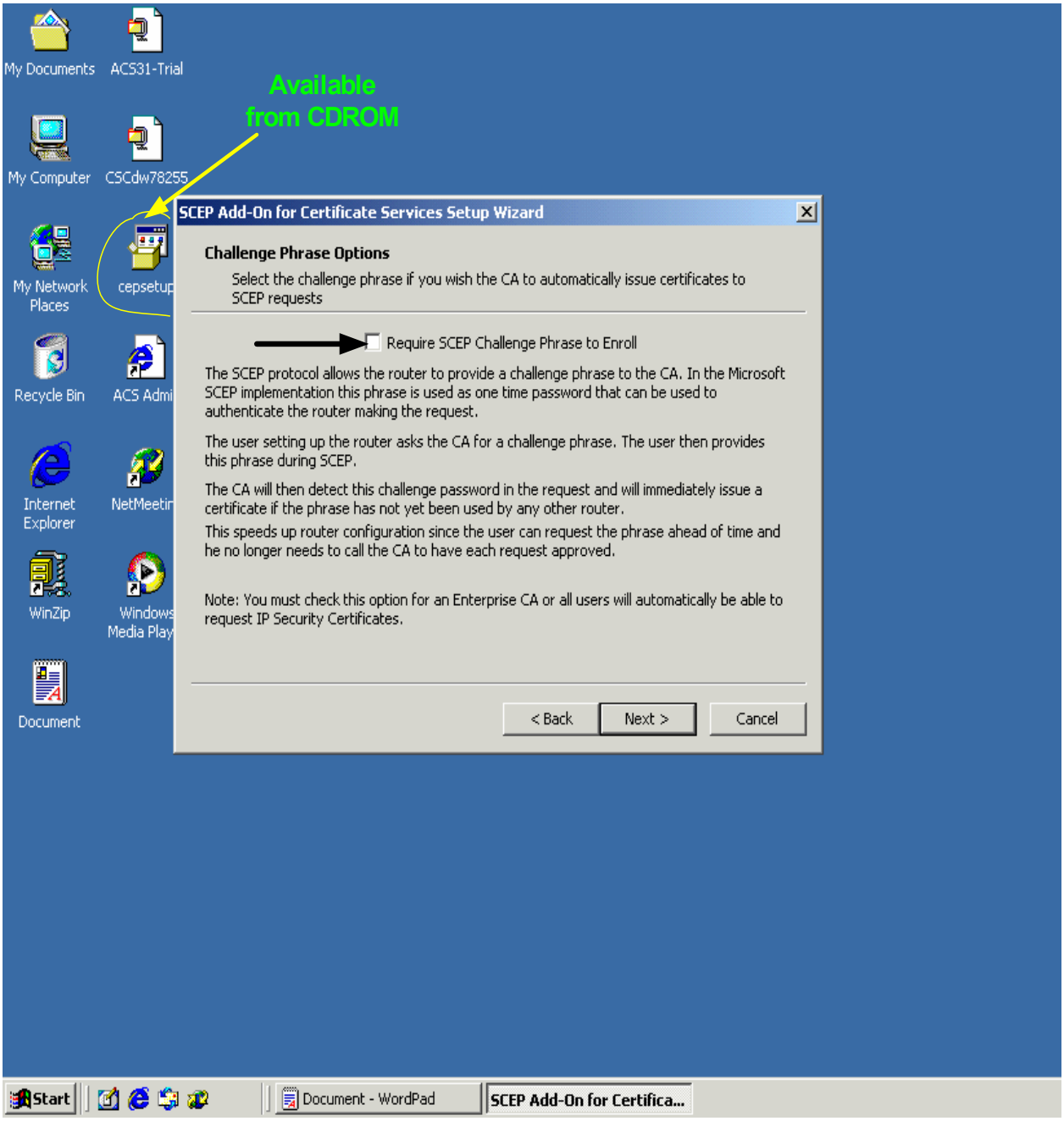
First, Install Microsoft CA / Win2k Server



Second, Install cepsetup.exe from CD



Note: Make sure to uncheck SCEP Challenge Phrase

Step 1
PIX2

```
domain-name cisco.com
clock set 08:11:00 1 april 2003
clock timezone GMT
ntp authentication-key 6727 md5 ********
ntp authenticate
ntp trusted-key 6727
ntp server 192.168.1.1 key 6727 source inside prefer
ntp server 192.168.1.7 key 6727 source inside
```

Step 2

```
ca generate rsa key 512
ca identity caserver 192.168.1.7:/certsrv/mscep/mscep.dll
ca configure caserver ra 20 1 crloptional
ca authen caserver
ca enroll caserver cisco
```

```
sho ca mypubkey rsa
% Key pair was generated at: 03:39:37 UTC Apr 2 2003
Key name: PIX2.cisco.com
 Usage: General Purpose Key
 Key Data:
  307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00910de3
3c9382a6
  49bb9beb a56ce6e1 1a016fac 73f32e58 de676b61 ff7ea679 625e37f8
38a7ff81
  38f79eae f3fba3be ff490ea1 bd7c3d04 7733f3ba 3f7320f2 66d46dbf
6851b387
  43bb9639 f4c22284 8555eff0 b905b716 285d44d0 bcc44b4d e3020301
0001
```

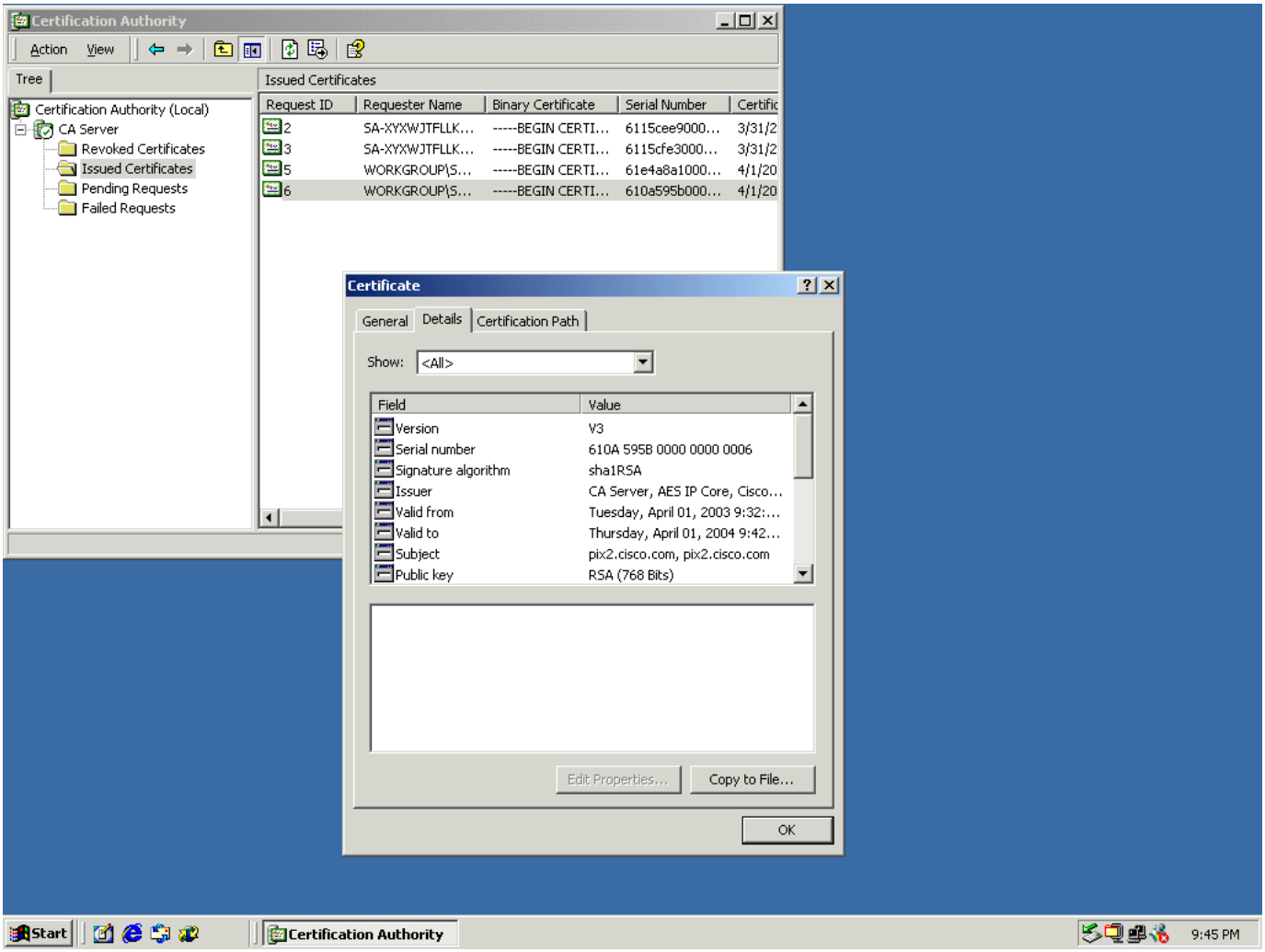
```
PIX2(config)# sho clock
03:46:32.112 UTC Wed Apr 2 2003
```

```
PIX2(config)# sho ca certificate
CA Certificate
  Status: Available
  Certificate Serial Number: 528fe682a3fb53bd4ec07eaa0d059380
  Key Usage: Signature
    CN = CA Server
    OU = AES IP Core
    O = "Cisco Systems
    Inc"
    L = San Jose
    ST = CA
    C = US
    EA =<16> ccie4460@hotmail.com
  Validity Date:
    start date: 23:12:01 UTC Mar 31 2003
    end   date: 23:20:53 UTC Mar 31 2005

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 6115cee9000000000002
  Key Usage: Signature
    CN = DB
    OU = dB
    O = DB
    L = db
    ST = WI
    C = US
    EA =<16> DB
  Validity Date:
    start date: 23:46:53 UTC Mar 31 2003
    end   date: 23:56:53 UTC Mar 31 2004

RA KeyEncipher Certificate
```

```
  Status: Available
  Certificate Serial Number: 6115cfe3000000000003
  Key Usage: Encryption
    CN = DB
    OU = dB
    O = DB
    L = db
    ST = WI
    C = US
    EA =<16> DB
  Validity Date:
    start date: 23:46:53 UTC Mar 31 2003
    end   date: 23:56:53 UTC Mar 31 2004

Certificate
  Subject Name
    Name: PIX2.cisco.com
  Status: Pending
  Key Usage: General Purpose
    Fingerprint:  00000000 00000000 00000000 00000000

PIX2(config)#     Fingerprint:  58c9eff9 d5885b15 47f90327
d7cb9815

The certificate has been granted by CA!
```

```
ca save all
write memory
```

Example from the CA Server




```
R5

clock timezone PST -8
clock summer-time PDT recurring
!
ntp authentication-key 1 md5 110A1A0C12 7
ntp authentication-key 6727 md5 03550B5F225F711C6F594F544F 7
ntp authenticate
ntp trusted-key 6727
ntp clock-period 17180064
ntp master
ntp peer 130.100.26.3 key 6727
```

```
R5#      sho clock
20:49:20.619 PST Tue Apr 1 2003
```

Note: Make sure that time is in sync with the CA Server

Step 3

```
R5(config)#ip domain-name cisco.com
R5(config)#crypto key generate rsa
The name for the keys will be: R5.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
```

```
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
00:45:12: %SSH-5-ENABLED: SSH 1.5 has been enabled

R5(ca-identity)#crypto ca identity caserver
R5(ca-identity)# enrollment mode ra
R5(ca-identity)#$ url
http://130.100.26.7:80/certsrv/mscep/mscep.dll
R5(ca-identity)# crl optional
```

Configure PIX2 to allow NTP and CA auth

```
PIX2
ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0

access-list outside_access_in permit tcp any host 130.100.26.7 eq
www
access-list outside_access_in permit udp any host 130.100.26.3 eq
ntp
static (inside,outside) 130.100.26.7 192.168.1.7 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.3 192.168.1.1 netmask
255.255.255.255 0 0

access-group outside_access_in in interface outside
```

```
From R5 to verify port 80'

telnet 130.100.26.7 80 <- test port 80

 HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 02 Apr 2003 06:22:32 GMT
Content-Length: 3167
```

```
clock timezone PST -8
clock summer-time PDT recurring
!
ntp authentication-key 6727 md5 03550B5F225F711C6F594F544F 7
ntp authenticate
ntp trusted-key 6727
ntp clock-period 17180064
ntp master
ntp peer 130.100.26.3 key 6727
!
R5#     sho clock
20:49:20.619 PST Tue Apr 1 2003
```

```
R5(config)#crypto ca authen caserver
Certificate has the following attributes:
Fingerprint: 5DD1A888 6F2BA9DA 9FF73BB7 CEC4499A
```

```
% Do you accept this certificate? [yes/no]:yes
```

```
R5(config)#crypto ca enroll caserver
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
   password to the CA Administrator in order to revoke your
certificate.
   For security reasons your password will not be saved in the
configuration.
   Please make a note of it.

Password:cisco
Re-enter password:cisco

% The subject name in the certificate will be: R5.cisco.com
% Include the router serial number in the subject name? [yes/no]:
yes
% The serial number in the certificate will be: 06904020
% Include an IP address in the subject name? [yes/no]: yes
Interface:
% Skipping IP address

Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the
fingerprint.
```

```
R5#sho crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 610FD716000000000007
  Key Usage: General Purpose
  Issuer:
    CN = CA Server
     OU = AES IP Core
     O = "Cisco Systems
     Inc"
     L = San Jose
     ST = CA
     C = US
     EA = ccie4460@hotmail.com
  Subject Name Contains:
    Name: R5.cisco.com
    Serial Number: 06904020
  CRL Distribution Point:
    http://sa-xyxwjtfllkbu/CertEnroll/CA%20Server.crl
  Validity Date:
    start date: 22:37:58 PST Apr 1 2003
    end   date: 22:47:58 PST Apr 1 2004
  Associated Identity: caserver

RA Signature Certificate
  Status: Available
```

```
  Certificate Serial Number: 6115CEE9000000000002
  Key Usage: Signature
  Issuer:
    CN = CA Server
     OU = AES IP Core
     O = "Cisco Systems
     Inc"
     L = San Jose
     ST = CA
     C = US
     EA = ccie4460@hotmail.com
  Subject:
    CN = DB
     OU = dB
     O = DB
     L = db
     ST = WI
     C = US
     EA = DB
  CRL Distribution Point:
    http://sa-xyxwjtfllkbu/CertEnroll/CA%20Server.crl
  Validity Date:
    start date: 15:46:53 PST Mar 31 2003
    end   date: 15:56:53 PST Mar 31 2004
  Associated Identity: caserver

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 6115CFE3000000000003
  Key Usage: Encryption
  Issuer:
    CN = CA Server
     OU = AES IP Core
     O = "Cisco Systems
     Inc"
     L = San Jose
     ST = CA
     C = US
     EA = ccie4460@hotmail.com
  Subject:
    CN = DB
     OU = dB
     O = DB
     L = db
     ST = WI
     C = US
     EA = DB
  CRL Distribution Point:
    http://sa-xyxwjtfllkbu/CertEnroll/CA%20Server.crl
  Validity Date:
    start date: 15:46:53 PST Mar 31 2003
    end   date: 15:56:53 PST Mar 31 2004
  Associated Identity: caserver

CA Certificate
  Status: Available
  Certificate Serial Number: 528FE682A3FB53BD4EC07EAA0D059380
  Key Usage: Signature
```

```
  Issuer:
    CN = CA Server
     OU = AES IP Core
     O = "Cisco Systems
     Inc"
     L = San Jose
     ST = CA
     C = US
     EA = ccie4460@hotmail.com
  Subject:
    CN = CA Server
     OU = AES IP Core
     O = "Cisco Systems
     Inc"
     L = San Jose
     ST = CA
     C = US
     EA = ccie4460@hotmail.com
  CRL Distribution Point:
    http://sa-xyxwjtfllkbu/CertEnroll/CA%20Server.crl
  Validity Date:
    start date: 15:12:01 PST Mar 31 2003
    end   date: 15:20:53 PST Mar 31 2005
  Associated Identity: caserver
```

Configuration for PIX2 VPN

PIX2 VPN Section Part of Step 2

```
access-list outside_access_in permit udp any host 130.100.26.3 eq
ntp
```

```
access-list inside_outbound_nat0_acl permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
access-list inside_outbound_nat0_acl permit ip 192.168.1.0
255.255.255.0 15.15.15.0 255.255.255.0
access-list outside_cryptomap_40 permit ip 192.168.1.0
255.255.255.0 15.15.15.0 255.255.255.0
```

```
global (outside) 10 interface
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 10 0.0.0.0 0.0.0.0 0 0
```

```
static (inside,outside) 130.100.26.7 192.168.1.7 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.8 192.168.1.8 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.3 192.168.1.1 netmask
255.255.255.255 0 0
```

```
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 130.100.26.6 1
route inside 192.168.0.0 255.255.0.0 192.168.1.1 1
```

```
ntp authentication-key 6727 md5 ********
ntp authenticate
ntp trusted-key 6727
```

```
ntp server 192.168.1.1 key 6727 source inside prefer
ntp server 192.168.1.7 key 6727 source inside
```

```
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 40 ipsec-isakmp
crypto map outside_map 40 match address outside_cryptomap_40
crypto map outside_map 40 set peer 140.100.56.5
crypto map outside_map 40 set transform-set ESP-DES-MD5
crypto map outside_map interface outside
isakmp enable outside
isakmp peer ip 140.100.45.5 no-xauth no-config-mode
isakmp policy 40 authentication rsa-sig
isakmp policy 40 encryption des
isakmp policy 40 hash md5
isakmp policy 40 group 1
isakmp policy 40 lifetime 86400
isakmp identity hostname
ca identity caserver 192.168.1.7:/certsrv/mscep/mscep.dll
ca configure caserver ra 20 1 crloptional
```

```
PIX2# sho crypto map

Crypto Map: "outside_map" interfaces: { outside }

Crypto Map "outside_map" 20 ipsec-isakmp
        Peer = 130.100.1.1
        access-list outside_cryptomap_20; 1 elements
        access-list outside_cryptomap_20 line 1 permit ip
192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0 (hitcnt=0)
        Current peer: 130.100.1.1
        Security association lifetime: 4608000 kilobytes/28800
seconds
        PFS (Y/N): N
        Transform sets={ ESP-DES-MD5, }

Crypto Map "outside_map" 40 ipsec-isakmp
        Peer = 140.100.56.5
        access-list outside_cryptomap_40; 1 elements
        access-list outside_cryptomap_40 line 1 permit ip
192.168.1.0 255.255.255.0 15.15.15.0 255.255.255.0 (hitcnt=6)
        Current peer: 140.100.56.5
        Security association lifetime: 4608000 kilobytes/28800
seconds
        PFS (Y/N): N
        Transform sets={ ESP-DES-MD5, }

Crypto Map: "vpn" interfaces: { }

Crypto Map "vpn" 10 ipsec-isakmp
        No matching address list set.
        Current peer: 0.0.0.0
        Security association lifetime: 4608000 kilobytes/28800
seconds
        PFS (Y/N): N
        Transform sets={ }
PIX2#
```

```
PIX2(config)# sho debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug crypto ca 1
PIX2(config)#
```

Ping from PC on Segment 192.168.1.x

```
C:\Documents and Settings\Admin>ping 15.15.15.15

Pinging 15.15.15.15 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 15.15.15.15: bytes=32 time=205ms TTL=255
Reply from 15.15.15.15: bytes=32 time=99ms TTL=255

Ping statistics for 15.15.15.15:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 205ms, Average = 152ms
```

```
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:140.100.56.5, dest:130.100.26.2
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 40 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65535
policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth RSA sig
```

```
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing RSA signature authentication using id type
ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:140.100.56.5, dest:130.100.26.2
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing CERT_REQ payload. message ID = 0
ISAKMP (0): peer wants a CT_X509_SIGNATURE cert
ISAKMP (0): processing CERT_REQ payload. message ID = 0
ISAKMP (0): peer wants a CT_X509_KEY_EXCHANGE cert
CRYPTO_CA: certificate not found
ISAKMP (0): can't find router cert for key exchange!
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): ID payload
        next-payload : 6
        type         : 2
        protocol     : 17
        port         : 500
        length       : 18
ISAKMP (0): Total payload length: 22
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:140.100.56.5, dest:130.100.26.2
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing CERT payload. message ID = 0
ISAKMP (0): processing a CT_X509_SIGNATURE cert
CRYPTO_PKI: status = 0: crl check ignored
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL

CRYPTO_PKI: cert revocation status unknown.
ISAKMP (0): cert approved with warning
ISAKMP (0): processing SIG payload. message ID = 0
ISAKMP (0): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn =
R5.cisco.com
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of
1118864114:42b082f2IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x3bf8a75a(1006151514) for SA
        from    140.100.56.5 to    130.100.26.2 for prot 3

return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:140.100.56.5/500 Total VPN
Peers:1
```

```
VPN Peer: ISAKMP: Peer ip:140.100.56.5/500 Ref cnt incremented
to:1 Total VPN Peers:1
crypto_isakmp_process_block:src:140.100.56.5, dest:130.100.26.2
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1118864114

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 140.100.56.5, src= 130.100.26.2,
    dest_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1118864114

ISAKMP (0): processing ID payload. message ID = 1118864114
ISAKMP (0): processing ID payload. message ID = 1118864114
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
        spi 828322018, message ID = 1118864114
ISAKMP (0): processing responder lifetime
ISAKMP (0): responder lifetime of 3600smap_alloc_entry: allocating
entry 1
map_alloc_entry: allocating entry 2

ISAKMP (0): Creating IPSec SAs
        inbound SA from    140.100.56.5 to    130.100.26.2 (proxy
15.15.15.0 to     192.168.1.0)
        has spi 1006151514 and conn_id 1 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        outbound SA from    130.100.26.2 to    140.100.56.5 (proxy
192.168.1.0 to      15.15.15.0)
        has spi 828322018 and conn_id 2 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a
queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 130.100.26.2, src= 140.100.56.5,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
```

```
    spi= 0x3bf8a75a(1006151514), conn_id= 1, keysize= 0, flags=
0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 130.100.26.2, dest= 140.100.56.5,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x315f30e2(828322018), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:140.100.56.5/500 Ref cnt incremented to:2
Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:140.100.56.5/500 Ref cnt incremented to:3
Total VPN Peers:1
return status is IKMP_NO_ERROR
```

```
PIX2(config)# sho crypto is sa
Total     : 2
Embryonic : 0
        dst               src        state     pending     created
    130.100.26.2     140.100.56.5    QM_IDLE         0           1
```

Configuration for R5 VPN

R5 VPN Section Part of Step 3

```
crypto isakmp policy 10
 hash md5
 authentication rsa-sig
!
!
crypto ipsec transform-set trvpn esp-des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 130.100.26.2
 set transform-set trvpn
 match address 101
!
interface Loopback15
Description VPN-Loopback To PIX2 CA Auth:
 ip address 15.15.15.15 255.255.255.0
!
interface Ethernet0
 ip address 130.100.26.5 255.255.255.224
 standby 1 ip 130.100.26.1
 standby 1 priority 95
```

```
 standby 1 preempt
 standby 1 authentication ccie
!
interface Serial1
 ip address 140.100.56.5 255.255.255.192
 ip access-group 100 in
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf network point-to-point
 clockrate 125000
 crypto map vpn
!
access-list 101 permit ip 15.15.15.0 0.0.0.255 192.168.1.0
0.0.0.255 log
```

```
R5#sho crypto map
Crypto Map "vpn" 10 ipsec-isakmp
        Peer = 130.100.26.2
        Extended IP access list 101
            access-list 101 permit ip 15.15.15.0 0.0.0.255
192.168.1.0 0.0.0.255
        Current peer: 130.100.26.2
        Security association lifetime: 4608000 kilobytes/3600
seconds
        PFS (Y/N): N
        Transform sets={ trvpn, }
        Interfaces using crypto map vpn:
                Ethernet0
                Serial1
```

Step 4

```
From PC on Segment 192.168.1.x
C:\Documents and Settings\Admin>ping 15.15.15.15

Pinging 15.15.15.15 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 15.15.15.15: bytes=32 time=24ms TTL=255
Reply from 15.15.15.15: bytes=32 time=24ms TTL=255

Ping statistics for 15.15.15.15:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 24ms, Average = 24ms

C:\Documents and Settings\Admin>
```

```
R5#
04:05:15: ISAKMP (0:0): received packet from 130.100.26.2 (N) NEW
SA
04:05:15: ISAKMP: local port 500, remote port 500
04:05:15: ISAKMP (0:3): processing SA payload. message ID = 0
04:05:15: ISAKMP (0:3): Checking ISAKMP transform 1 against
priority 10 policy
04:05:15: ISAKMP:      encryption DES-CBC
04:05:15: ISAKMP:      hash MD5
04:05:15: ISAKMP:      default group 1
04:05:15: ISAKMP:      auth RSA sig
04:05:15: ISAKMP:      life type in seconds
04:05:15: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
04:05:15: ISAKMP (0:3): Authentication method offered does not
match policy!
04:05:15: ISAKMP (0:3): atts are not acceptable. Next payload is 3
04:05:15: ISAKMP (0:3): Checking ISAKMP transform 2 against
priority 10 policy
04:05:15: ISAKMP:      encryption DES-CBC
04:05:15: ISAKMP:      hash SHA
04:05:15: ISAKMP:      default group 1
04:05:15: ISAKMP:      auth RSA sig
04:05:15: ISAKMP:      life type in seconds
04:05:15: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
04:05:15: ISAKMP (0:3): Hash algorithm offered does not match
policy!
04:05:15: ISAKMP (0:3): atts are not acceptable. Next payload is 0
04:05:15: ISAKMP (0:3): Checking ISAKMP transform 1 against
priority 65535 policy
04:05:15: ISAKMP:      encryption DES-CBC
04:05:15: ISAKMP:      hash MD5
04:05:15: ISAKMP:      default group 1
04:05:15: ISAKMP:      auth RSA sig
04:05:15: ISAKMP:      life type in seconds
04:05:15: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
04:05:15: ISAKMP (0:3): Hash algorithm offered does not match
policy!
04:05:15: ISAKMP (0:3): atts are not acceptable. Next payload is 3
04:05:15: ISAKMP (0:3): Checking ISAKMP transform 2 against
priority 65535 policy
04:05:15: ISAKMP:      encryption DES-CBC
04:05:15: ISAKMP:      hash SHA
04:05:15: ISAKMP:      default group 1
04:05:15: ISAKMP:      auth RSA sig
04:05:15: ISAKMP:      life type in seconds
04:05:15: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
04:05:15: ISAKMP (0:3): atts are acceptable. Next payload is 0
04:05:15: CryptoEngine0: generate alg parameter
04:05:16: CRYPTO_ENGINE: Dh phase 1 status: 0
04:05:16: CRYPTO_ENGINE: Dh phase 1 status: 0
04:05:16: ISAKMP (3): My ID configured as IPv4 Addr,but Addr not
in Cert!
04:05:16: ISAKMP (3): Using FQDN as My ID
04:05:16: ISAKMP (0:3): SA is doing RSA signature authentication
using id type ID_FQDN
04:05:16: ISAKMP (0:3): sending packet to 130.100.26.2 (R)
MM_SA_SETUP
```

```
04:05:16: ISAKMP (0:3): received packet from 130.100.26.2 (R)
MM_SA_SETUP
04:05:16: ISAKMP (0:3): processing KE payload. message ID = 0
04:05:16: CryptoEngine0: generate alg parameter
04:05:18: ISAKMP (0:3): processing NONCE payload. message ID = 0
04:05:19: CryptoEngine0: calculate pkey hmac for conn id 3
04:05:19: CryptoEngine0: create ISAKMP SKEYID for conn id 3
04:05:19: ISAKMP (0:3): SKEYID state generated
04:05:19: ISAKMP (0:3): processing CERT_REQ payload. message ID =
0
04:05:19: ISAKMP (0:3): peer wants a CT_X509_SIGNATURE cert
04:05:19: ISAKMP (0:3): peer want cert issued by CN = CA Server,
OU = AES IP Core, O = "Cisco Systems, Inc", L =

San Jose
, ST = CA, C = US, EA = ccie4460@hotmail.com
04:05:19: ISAKMP (0:3): processing vendor id payload
04:05:19: ISAKMP (0:3): processing vendor id payload
04:05:19: ISAKMP (0:3): processing vendor id payload
04:05:19: ISAKMP (0:3): processing vendor id payload
04:05:19: ISAKMP (0:3): speaking to another IOS box!
04:05:19: ISAKMP (0:3): sending packet to 130.100.26.2 (R)
MM_KEY_EXCH
04:05:19: ISAKMP (0:3): received packet from 130.100.26.2 (R)
MM_KEY_EXCH
04:05:19: ISAKMP (0:3): processing ID payload. message ID = 0
04:05:19: ISAKMP (0:3): processing CERT payload. message ID = 0
04:05:19: ISAKMP (0:3): processing a CT_X509_SIGNATURE cert
04:05:19: CRYPTO_ENGINE: key process suspended and continued
04:05:19: ISAKMP (0:3): cert approved with warning
04:05:20: ISAKMP (0:3): processing SIG payload. message ID = 0
04:05:20: ISAKMP (3): sa->peer.name = , sa-
>peer_id.id.id_fqdn.fqdn = PIX2.cisco.com
04:05:20: Crypto engine 0: RSA decrypt with public key
04:05:20: CryptoEngine0: CRYPTO_RSA_PUB_DECRYPT
04:05:20: CRYPTO_ENGINE: key process suspended and continued
04:05:20: CryptoEngine0: generate hmac context for conn id 3
04:05:20: ISAKMP (0:3): SA has been authenticated with
130.100.26.2
04:05:20: ISAKMP (3): ID payload
        next-payload : 6
        type         : 2
        protocol     : 17
        port         : 500
        length       : 12
04:05:20: ISAKMP (3): Total payload length: 16
04:05:20: ISKAMP: growing send buffer from 1024 to 3072
04:05:20: -Traceback= 3C2F482 3C38180 3C38412 3C2DCEA 3C27972
3C28892
04:05:20: CryptoEngine0: generate hmac context for conn id 3
04:05:20: Crypto engine 0: RSA encrypt with private key
04:05:20: CryptoEngine0: CRYPTO_RSA_PRIV_ENCRYPT
04:05:22: CRYPTO_ENGINE: key process suspended and continued
04:05:22: CRYPTO_ENGINE: key process suspended and continued
04:05:22: CRYPTO_ENGINE: key process suspended and continued
04:05:22: CRYPTO_ENGINE: key process suspended and continued
04:05:23: CRYPTO_ENGINE: key process suspended and continued
04:05:23: CRYPTO_ENGINE: key process suspended and continued
```

```
04:05:23: CRYPTO_ENGINE: key process suspended and continued
04:05:23: CRYPTO_ENGINE: key process suspended and continued
04:05:23: CryptoEngine0: clear dh number for conn id 1
04:05:23: ISAKMP (0:3): sending packet to 130.100.26.2 (R) QM_IDLE
04:05:23: ISAKMP (0:3): received packet from 130.100.26.2 (R)
QM_IDLE
04:05:23: CryptoEngine0: generate hmac context for conn id 3
04:05:23: ISAKMP (0:3): processing HASH payload. message ID = -
688079982
04:05:23: ISAKMP (0:3): processing NOTIFY INITIAL_CONTACT protocol
1
        spi 0, message ID = -688079982, sa = 81377C
04:05:23: ISAKMP (0:3): deleting node -688079982 error FALSE
reason "informational (in) state 1"
04:05:23: ISAKMP (0:3): received packet from 130.100.26.2 (R)
QM_IDLE
04:05:23: CryptoEngine0: generate hmac context for conn id 3
04:05:23: ISAKMP (0:3): processing HASH payload. message ID =
720620234
04:05:23: ISAKMP (0:3): processing SA payload. message ID =
720620234
04:05:23: ISAKMP (0:3): Checking IPSec proposal 1
04:05:23: ISAKMP: transform 1, ESP_DES
04:05:23: ISAKMP:   attributes in transform:
04:05:23: ISAKMP:      encaps is 1
04:05:23: ISAKMP:      SA life type in seconds
04:05:23: ISAKMP:      SA life duration (basic) of 28800
04:05:23: ISAKMP:      SA life type in kilobytes
04:05:23: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50
0x0
04:05:24: ISAKMP:      authenticator is HMAC-MD5
04:05:24: validate proposal 0
04:05:24: ISAKMP (0:3): atts are acceptable.
04:05:24: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 140.100.56.5, remote=
130.100.26.2,
    local_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
04:05:24: validate proposal request 0
04:05:24: ISAKMP (0:3): processing NONCE payload. message ID =
720620234
04:05:24: ISAKMP (0:3): processing ID payload. message ID =
720620234
04:05:24: ISAKMP (0:3): processing ID payload. message ID =
720620234
04:05:24: ISAKMP (0:3): asking for 1 spis from ipsec
04:05:24: IPSEC(key_engine): got a queue event...
04:05:24: IPSEC(spi_response): getting spi 1571703012 for SA
        from 140.100.56.5    to 130.100.26.2    for prot 3
04:05:24: ISAKMP: received ke message (2/1)
04:05:24: CryptoEngine0: generate hmac context for conn id 3
04:05:24: ISAKMP (0:3): sending packet to 130.100.26.2 (R) QM_IDLE
04:05:24: ISAKMP (0:3): received packet from 130.100.26.2 (R)
QM_IDLE
04:05:24: CryptoEngine0: generate hmac context for conn id 3
```

```
04:05:24: ipsec allocate flow 0
04:05:24: ipsec allocate flow 0
04:05:24: ISAKMP (0:3): Creating IPSec SAs
04:05:24:         inbound SA from 130.100.26.2 to 140.100.56.5
        (proxy 192.168.1.0 to 15.15.15.0)
04:05:24:         has spi 0x5DAE48E4 and conn_id 2004 and flags 4
04:05:24:         lifetime of 28800 seconds
04:05:24:         lifetime of 4608000 kilobytes
04:05:24:         outbound SA from 140.100.56.5    to 130.100.26.2
(proxy 15.15.15.0      to 192.168.1.0    )
04:05:24:         has spi 1382175893 and conn_id 2005 and flags C
04:05:24:         lifetime of 28800 seconds
04:05:24:         lifetime of 4608000 kilobytes
04:05:24: ISAKMP (0:3): deleting node 720620234 error FALSE reason
"quick mode done (await()"
04:05:24: IPSEC(key_engine): got a queue event...
04:05:24: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 140.100.56.5, remote=
130.100.26.2,
    local_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x5DAE48E4(1571703012), conn_id= 2004, keysize= 0, flags=
0x4
04:05:24: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 140.100.56.5, remote=
130.100.26.2,
    local_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x52625495(1382175893), conn_id= 2005, keysize= 0, flags=
0xC
04:05:24: IPSEC(create_sa): sa created,
  (sa) sa_dest= 140.100.56.5, sa_prot= 50,
    sa_spi= 0x5DAE48E4(1571703012),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2004
04:05:24: IPSEC(create_sa): sa created,
  (sa) sa_dest= 130.100.26.2, sa_prot= 50,
    sa_spi= 0x52625495(1382175893),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2005
04:05:24: IPSEC(add_sa): peer asks for new SAs -- expire current
in 120 sec.,
  (sa) sa_dest= 130.100.26.2, sa_prot= 50,
    sa_spi= 0x3BF8A75A(1006151514),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2003,
  (identity) local= 140.100.56.5, remote= 130.100.26.2,
    local_proxy= 15.15.15.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4)
```

```
R5#sho crypto engine connections active
  ID Interface       IP-Address      State  Algorithm
Encrypt  Decrypt
   1 <none>          <none>          set    HMAC_SHA+DES_56_CB
0        0
```

```
   2 Serial1          140.100.56.5    set    HMAC_SHA+DES_56_CB
0         0
   3 Serial1          140.100.56.5    set    HMAC_SHA+DES_56_CB
0         0
2004 Serial1          140.100.56.5    set    HMAC_MD5+DES_56_CB
0         2
2005 Serial1          140.100.56.5    set    HMAC_MD5+DES_56_CB
2         0
```

```
R5#sho access-lists 101
Extended IP access list 101
    permit ip 15.15.15.0 0.0.0.255 192.168.1.0 0.0.0.255 log (56
matches)
```

Full configuration of R5

```
R5#sho run
Building configuration...

Current configuration : 13174 bytes
!
! Last configuration change at 22:42:00 PST Tue Apr 1 2003
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R5
!
logging queue-limit 100
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip domain-name cisco.com
!
!
crypto ca identity caserver
 enrollment mode ra
 enrollment url http://130.100.26.7:80/certsrv/mscep/mscep.dll
 crl optional
crypto ca certificate chain caserver
 certificate 610FD716000000000007
  30820413 308203BD A0030201 02020A61 0FD71600 00000000 07300D06
092A8648
  86F70D01 01050500 30819931 23302106 092A8648 86F70D01 09011614
63636965
  34343630 40686F74 6D61696C 2E636F6D 310B3009 06035504 06130255
53310B30
  09060355 04081302 43413111 300F0603 55040713 0853616E 204A6F73
65311B30
  19060355 040A1312 43697363 6F205379 7374656D 732C2049 6E633114
30120603
```

```
  55040B13 0B414553 20495020 436F7265 31123010 06035504 03130943
41205365
  72766572 301E170D 30333034 30323036 33373538 5A170D30 34303430
32303634
  3735385A 302B3110 300E0603 55040513 07363930 34303230 31173015
06092A86
  4886F70D 01090213 0872352E 63697363 6F305C30 0D06092A 864886F7
0D010101
  0500034B 00304802 4100B6F1 9D40EFB2 0F3A1DF1 272B029E CACEC9E2
E83FA4AD
  E385D968 64296D58 5526AFEC 0C614F53 3E08169E DE058C55 A895A4B9
97489C47
  4D90A898 12439BA4 8F630203 010001A3 82025230 82024E30 0B060355
1D0F0404
  030205A0 301D0603 551D0E04 160414D1 114FC3DF 929B5C02 2388AB59
306286C2
  113A0230 81D50603 551D2304 81CD3081 CA801469 5E123437 AE0ACEF7
B9203CD4
  36CFFF22 02CE6DA1 819FA481 9C308199 31233021 06092A86 4886F70D
01090116
  14636369 65343436 3040686F 746D6169 6C2E636F 6D310B30 09060355
04061302
  5553310B 30090603 55040813 02434131 11300F06 03550407 13085361
6E204A6F
  7365311B 30190603 55040A13 12436973 636F2053 79737465 6D732C20
496E6331
  14301206 0355040B 130B4145 53204950 20436F72 65311230 10060355
04031309
  43412053 65727665 72821052 8FE682A3 FB53BD4E C07EAA0D 05938030
16060355
  1D110101 FF040C30 0A820872 352E6369 73636F30 7D060355 1D1F0476
30743037
  A035A033 86316874 74703A2F 2F73612D 78797877 6A74666C 6C6B6275
2F436572
  74456E72 6F6C6C2F 43412532 30536572 7665722E 63726C30 39A037A0
35863366
  696C653A 2F2F5C5C 73612D78 7978776A 74666C6C 6B62755C 43657274
456E726F
  6C6C5C43 41253230 53657276 65722E63 726C3081 B006082B 06010505
07010104
  81A33081 A0304D06 082B0601 05050730 02864168 7474703A 2F2F7361
2D787978
  776A7466 6C6C6B62 752F4365 7274456E 726F6C6C 2F73612D 78797877
6A74666C
  6C6B6275 5F434125 32305365 72766572 2E637274 304F0608 2B060105
05073002
  86436669 6C653A2F 2F5C5C73 612D7879 78776A74 666C6C6B 62755C43
65727445
  6E726F6C 6C5C7361 2D787978 776A7466 6C6C6B62 755F4341 25323053
65727665
  722E6372 74300D06 092A8648 86F70D01 01050500 03410042 8119C875
CC36535A
  2D13739E 7D975518 A93A0E81 7865864F 958C7EA7 46DB790C A3A231FC
C6A51E3F
  54C525B0 B13FA01C 61E21792 040168D4 565FD430 8ED599
  quit
 certificate ra-sign 6115CEE9000000000002
```

```
  3082048F 30820439 A0030201 02020A61 15CEE900 00000000 02300D06
092A8648
  86F70D01 01050500 30819931 23302106 092A8648 86F70D01 09011614
63636965
  34343630 40686F74 6D61696C 2E636F6D 310B3009 06035504 06130255
53310B30
  09060355 04081302 43413111 300F0603 55040713 0853616E 204A6F73
65311B30
  19060355 040A1312 43697363 6F205379 7374656D 732C2049 6E633114
30120603
  55040B13 0B414553 20495020 436F7265 31123010 06035504 03130943
41205365
  72766572 301E170D 30333033 33313233 34363533 5A170D30 34303333
31323335
  3635335A 30613111 300F0609 2A864886 F70D0109 01160244 42310B30
09060355
  04061302 5553310B 30090603 55040813 02574931 0B300906 03550407
13026462
  310B3009 06035504 0A130244 42310B30 09060355 040B1302 6442310B
30090603
  55040313 02444230 819F300D 06092A86 4886F70D 01010105 0003818D
00308189
  02818100 F0AAB4DB 414134F6 870C3C49 29E858C4 E0F3CF0E 9375BDAC
FB3C0C2E
  5AB32785 A2551672 040FAA47 A04AA851 4541D1C9 0D4A5BC6 37828D02
5A89640A
  2BF393DF 1E16D276 298EE699 B2651780 32ABA016 93836DF9 AB0310D7
3190AEBB
  7813E7E5 C73BE09D 5CB85BE3 4A19A1C9 4B1F0AED 67D8E6C7 70FDE2B7
055DCEF8
  103AADBF 02030100 01A38202 54308202 50300E06 03551D0F 0101FF04
04030206
  C0301506 03551D25 040E300C 060A2B06 01040182 37140201 301D0603
551D0E04
  16041464 A23711E7 273627D8 57898751 364637C3 4C4EA130 81D50603
551D2304
  81CD3081 CA801469 5E123437 AE0ACEF7 B9203CD4 36CFFF22 02CE6DA1
819FA481
  9C308199 31233021 06092A86 4886F70D 01090116 14636369 65343436
3040686F
  746D6169 6C2E636F 6D310B30 09060355 04061302 5553310B 30090603
55040813
  02434131 11300F06 03550407 13085361 6E204A6F 7365311B 30190603
55040A13
  12436973 636F2053 79737465 6D732C20 496E6331 14301206 0355040B
130B4145
  53204950 20436F72 65311230 10060355 04031309 43412053 65727665
72821052
  8FE682A3 FB53BD4E C07EAA0D 05938030 7D060355 1D1F0476 30743037
A035A033
  86316874 74703A2F 2F73612D 78797877 6A74666C 6C6B6275 2F436572
74456E72
  6F6C6C2F 43412532 30536572 7665722E 63726C30 39A037A0 35863366
696C653A
  2F2F5C5C 73612D78 7978776A 74666C6C 6B62755C 43657274 456E726F
6C6C5C43
  41253230 53657276 65722E63 726C3081 B006082B 06010505 07010104
81A33081
```

```
  A0304D06 082B0601 05050730 02864168 7474703A 2F2F7361 2D787978
776A7466
  6C6C6B62 752F4365 7274456E 726F6C6C 2F73612D 78797877 6A74666C
6C6B6275
  5F434125 32305365 72766572 2E637274 304F0608 2B060105 05073002
86436669
  6C653A2F 2F5C5C73 612D7879 78776A74 666C6C6B 62755C43 65727445
6E726F6C
  6C5C7361 2D787978 776A7466 6C6C6B62 755F4341 25323053 65727665
722E6372
  74300D06 092A8648 86F70D01 01050500 03410089 9D26160C 3EF11CF5
4632C7C0
  35DFFBD3 E801BFD3 24EF3658 F4F5FB7F 2B705820 4536C340 B4E09B0C
845BA40D
  63D9B822 80A46048 365F03E6 E0C17A34 C4F46C
  quit
 certificate ra-encrypt 6115CFE3000000000003
  3082048F 30820439 A0030201 02020A61 15CFE300 00000000 03300D06
092A8648
  86F70D01 01050500 30819931 23302106 092A8648 86F70D01 09011614
63636965
  34343630 40686F74 6D61696C 2E636F6D 310B3009 06035504 06130255
53310B30
  09060355 04081302 43413111 300F0603 55040713 0853616E 204A6F73
65311B30
  19060355 040A1312 43697363 6F205379 7374656D 732C2049 6E633114
30120603
  55040B13 0B414553 20495020 436F7265 31123010 06035504 03130943
41205365
  72766572 301E170D 30333033 33313233 34363533 5A170D30 34303333
31323335
  3635335A 30613111 300F0609 2A864886 F70D0109 01160244 42310B30
09060355
  04061302 5553310B 30090603 55040813 02574931 0B300906 03550407
13026462
  310B3009 06035504 0A130244 42310B30 09060355 040B1302 6442310B
30090603
  55040313 02444230 819F300D 06092A86 4886F70D 01010105 0003818D
00308189
  02818100 EB65C003 F9367673 D7C28900 6893DE5C 7A6BEBC1 A33F96B9
8F681663
  7DFFA61F 9127C18D C03D4663 743D2C54 39953B62 769FD388 C2AAF88F
FC9A984E
  3EBD9E45 35E70264 EE2F5382 9F1B29A6 35B4E191 78964491 920A5C87
2AEA05B1
  F85D1FC3 D55678AA BFF074C4 21E8DD89 41B69DB4 A0A5024C 1DC7326D
FC85CEBD
  4831D9A3 02030100 01A38202 54308202 50300E06 03551D0F 0101FF04
04030204
  30301506 03551D25 040E300C 060A2B06 01040182 37140201 301D0603
551D0E04
  16041462 53DAFB8E C3C14CB5 F7DB4E1C 95B9FFA5 C3B9C530 81D50603
551D2304
  81CD3081 CA801469 5E123437 AE0ACEF7 B9203CD4 36CFFF22 02CE6DA1
819FA481
  9C308199 31233021 06092A86 4886F70D 01090116 14636369 65343436
3040686F
```

```
  746D6169 6C2E636F 6D310B30 09060355 04061302 5553310B 30090603
55040813
  02434131 11300F06 03550407 13085361 6E204A6F 7365311B 30190603
55040A13
  12436973 636F2053 79737465 6D732C20 496E6331 14301206 0355040B
130B4145
  53204950 20436F72 65311230 10060355 04031309 43412053 65727665
72821052
  8FE682A3 FB53BD4E C07EAA0D 05938030 7D060355 1D1F0476 30743037
A035A033
  86316874 74703A2F 2F73612D 78797877 6A74666C 6C6B6275 2F436572
74456E72
  6F6C6C2F 43412532 30536572 7665722E 63726C30 39A037A0 35863366
696C653A
  2F2F5C5C 73612D78 7978776A 74666C6C 6B62755C 43657274 456E726F
6C6C5C43
  41253230 53657276 65722E63 726C3081 B006082B 06010505 07010104
81A33081
  A0304D06 082B0601 05050730 02864168 7474703A 2F2F7361 2D787978
776A7466
  6C6C6B62 752F4365 7274456E 726F6C6C 2F73612D 78797877 6A74666C
6C6B6275
  5F434125 32305365 72766572 2E637274 304F0608 2B060105 05073002
86436669
  6C653A2F 2F5C5C73 612D7879 78776A74 666C6C6B 62755C43 65727445
6E726F6C
  6C5C7361 2D787978 776A7466 6C6C6B62 755F4341 25323053 65727665
722E6372
  74300D06 092A8648 86F70D01 01050500 034100A9 6A08A206 0F354CFD
244DDEAA
  D2D7E870 1A88B53D 26359C95 15E75138 787AEB74 E01230EF 76549499
942A3536
  D70EF33B 6BFE249F 73243A7E 8C482521 FBF768
  quit
 certificate ca 528FE682A3FB53BD4EC07EAA0D059380
  30820306 308202B0 A0030201 02021052 8FE682A3 FB53BD4E C07EAA0D
05938030
  0D06092A 864886F7 0D010105 05003081 99312330 2106092A 864886F7
0D010901
  16146363 69653434 36304068 6F746D61 696C2E63 6F6D310B 30090603
55040613
  02555331 0B300906 03550408 13024341 3111300F 06035504 07130853
616E204A
  6F736531 1B301906 0355040A 13124369 73636F20 53797374 656D732C
20496E63
  31143012 06035504 0B130B41 45532049 5020436F 72653112 30100603
55040313
  09434120 53657276 6572301E 170D3033 30333331 32333132 30315A17
0D303530
  33333132 33323035 335A3081 99312330 2106092A 864886F7 0D010901
16146363
  69653434 36304068 6F746D61 696C2E63 6F6D310B 30090603 55040613
02555331
  0B300906 03550408 13024341 3111300F 06035504 07130853 616E204A
6F736531
  1B301906 0355040A 13124369 73636F20 53797374 656D732C 20496E63
31143012
```

```
  06035504 0B130B41 45532049 5020436F 72653112 30100603 55040313
09434120
  53657276 6572305C 300D0609 2A864886 F70D0101 01050003 4B003048
024100BF
  AD50953C 53538A7B B319588E A72A560E 1889E291 A4E37763 0D5CDC56
3558569B
  ED9F875D 2AE57CCC 573178E6 5E306478 91E177D3 09A30916 AD2B64E3
96E5B302
  03010001 A381D130 81CE300B 0603551D 0F040403 0201C630 0F060355
1D130101
  FF040530 030101FF 301D0603 551D0E04 16041469 5E123437 AE0ACEF7
B9203CD4
  36CFFF22 02CE6D30 7D060355 1D1F0476 30743037 A035A033 86316874
74703A2F
  2F73612D 78797877 6A74666C 6C6B6275 2F436572 74456E72 6F6C6C2F
43412532
  30536572 7665722E 63726C30 39A037A0 35863366 696C653A 2F2F5C5C
73612D78
  7978776A 74666C6C 6B62755C 43657274 456E726F 6C6C5C43 41253230
53657276
  65722E63 726C3010 06092B06 01040182 37150104 03020100 300D0609
2A864886
  F70D0101 05050003 4100B71E DABB567C 90497816 C2CF5262 ED2C0CAF
CBAA07E1
  B695AC94 4250AB2E D554C085 B3037F73 3F572938 A4645F2C E7AA2793
93FFC1F6
  61F2EA0D B9B2127C 2206
  quit
!
crypto isakmp policy 10
 hash md5
 authentication rsa-sig
!
!
crypto ipsec transform-set trvpn esp-des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 130.100.26.2
 set transform-set trvpn
 match address 101
!
!
!
!
interface Loopback5
 description OSPF Loopback
 ip address 5.5.5.5 255.255.255.255
!
interface Loopback15
 ip address 15.15.15.15 255.255.255.0
!
interface Loopback55
 description BGP Loopback
 ip address 5.5.5.55 255.255.255.255
!
interface Ethernet0
 ip address 130.100.26.5 255.255.255.224
 standby 1 ip 130.100.26.1
```

```
 standby 1 priority 95
 standby 1 preempt
 standby 1 authentication ccie
 crypto map vpn
!
interface Serial0
 ip address 140.100.45.5 255.255.255.192
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf network point-to-point
 fair-queue
!
interface Serial1
 ip address 140.100.56.5 255.255.255.192
 ip access-group 100 in
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf network point-to-point
 clockrate 125000
 crypto map vpn
!
router eigrp 5
 network 130.100.55.0 0.0.0.255
 no auto-summary
 no eigrp log-neighbor-changes
!
router ospf 123
 router-id 5.5.5.5
 log-adjacency-changes detail
 area 0 authentication message-digest
 area 45 authentication message-digest
 area 45 virtual-link 4.4.4.4 authentication message-digest
 area 45 virtual-link 4.4.4.4 message-digest-key 5 md5 cisco
 area 56 authentication message-digest
 area 56 virtual-link 6.6.6.6 authentication message-digest
 area 56 virtual-link 6.6.6.6 message-digest-key 5 md5 cisco
 redistribute eigrp 5 subnets
 network 5.5.5.5 0.0.0.0 area 45
 network 140.100.45.0 0.0.0.63 area 45
 network 140.100.56.0 0.0.0.63 area 56
!
router bgp 456
 no synchronization
 bgp router-id 5.5.5.5
 bgp cluster-id 84215095
 bgp log-neighbor-changes
 network 5.5.5.55 mask 255.255.255.255
 neighbor 140.100.45.4 remote-as 456
 neighbor 140.100.45.4 route-reflector-client
 neighbor 140.100.45.4 next-hop-self
 neighbor 140.100.56.6 remote-as 456
 neighbor 140.100.56.6 route-reflector-client
 neighbor 140.100.56.6 next-hop-self
 no auto-summary
!
ip classless
ip http server
!
```

```
access-list 100 deny   udp host 140.100.56.6 any eq 33434
access-list 100 permit ip any any
access-list 100 permit esp any any log
access-list 101 permit ip 15.15.15.0 0.0.0.255 192.168.1.0
0.0.0.255 log
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 privilege level 15
 no login
!
ntp authentication-key 6727 md5 03550B5F225F711C6F594F544F 7
ntp authenticate
ntp trusted-key 6727
ntp clock-period 17180064
ntp master
ntp peer 130.100.26.3 key 6727 prefer
end

R5#
```

Full configuration of PIX2

```
PIX2# sho run
: Saved
:
PIX Version 6.2(2)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX2
domain-name cisco.com
access-list outside_access_in permit udp any host 130.100.26.3 eq
ntp
access-list inside_outbound_nat0_acl permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
access-list inside_outbound_nat0_acl permit ip 192.168.1.0
255.255.255.0 15.15.15.0 255.255.255.0
access-list outside_cryptomap_20 permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
access-list outside_cryptomap_40 permit ip 192.168.1.0
255.255.255.0 15.15.15.0 255.255.255.0
ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0
global (outside) 10 interface
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 10 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 130.100.26.7 192.168.1.7 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.8 192.168.1.8 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.3 192.168.1.1 netmask
255.255.255.255 0 0
access-group outside_access_in in interface outside
```

```
route outside 0.0.0.0 0.0.0.0 130.100.26.6 1

ntp authentication-key 6727 md5 ********
ntp authenticate
ntp trusted-key 6727
ntp server 192.168.1.1 key 6727 source inside prefer
ntp server 192.168.1.7 key 6727 source inside prefer
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set trvpn esp-des
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 130.100.1.1
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map 40 ipsec-isakmp
crypto map outside_map 40 match address outside_cryptomap_40
crypto map outside_map 40 set peer 140.100.56.5
crypto map outside_map 40 set transform-set ESP-DES-MD5
crypto map outside_map interface outside

isakmp enable outside

isakmp key ******** address 140.100.45.5 netmask 255.255.255.255
no-xauth no-config-mode
isakmp peer ip 140.100.45.5 no-xauth no-config-mode
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
isakmp policy 40 authentication rsa-sig
isakmp policy 40 encryption des
isakmp policy 40 hash md5
isakmp policy 40 group 1
isakmp policy 40 lifetime 86400
ca identity caserver 192.168.1.7:/certsrv/mscep/mscep.dll
ca configure caserver ra 20 1 crloptional
```