PIX 6.x: Simple PIX−to−PIX VPN Tunnel Configuration Example

Document ID: 6211

Interactive: **This document offers customized analysis of your Cisco device.**

Contents

Introduction

This configuration allows two Cisco Secure PIX Firewalls to run a simple virtual private network (VPN) tunnel from PIX to PIX over the Internet or any public network that uses IP security (IPSec). IPSec is a combination of open standards that provides data confidentiality, data integrity, and data origin authentication between IPSec peers.

Refer to PIX/ASA 7.x: Simple PIX−to−PIX VPN Tunnel Configuration Example for more information on the same scenario where the Cisco Security appliance runs software version 7.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure PIX 515E Firewall with software version 6.3(5)
- Cisco Secure PIX 515E Firewall with software version 6.3(5)

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

IPSec negotiation can be broken down into five steps, which includes two Internet Key Exchange (IKE) phases.

1. An IPSec tunnel is initiated by interesting traffic. Traffic is considered interesting when it travels between the IPSec peers.
2. In IKE Phase 1, the IPSec peers negotiate the established IKE Security Association (SA) policy. Once the peers are authenticated, a secure tunnel is created using Internet Security Association and Key Management Protocol (ISAKMP).
3. In IKE Phase 2, the IPSec peers use the authenticated and secure tunnel to negotiate IPSec SA transforms. The negotiation of the shared policy determines how the IPSec tunnel is established.
4. The IPSec tunnel is created and data is transferred between the IPSec peers based on the IPSec parameters configured in the IPSec transform sets.
5. The IPSec tunnel terminates when the IPSec SAs are deleted or when their lifetime expires.

Note: IPSec negotiation between the two PIXs fails if the SAs on both of the IKE phases do not match on the peers.
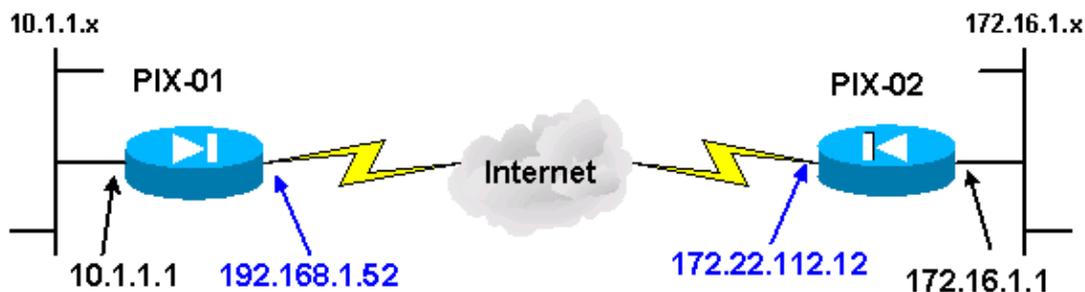
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) for more information on the commands used in this document.

Network Diagram

This document uses this network diagram:

Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. These are RFC 1918 addresses which have been used in a lab environment.

IKE and IPSec Configuration

The IPSec configuration on each PIX only varies when you insert the peer information and the naming convention chosen for the crypto maps and transform sets. The configuration can be verified with the **write terminal** or **show** commands. The relevant commands are **show isakmp**, **show isakmp policy**, **show**

access−list, **show crypto IPSec transform−set**, and **show crypto map**. Refer to Cisco Secure PIX Firewall Command References for more information on these commands.

Complete these steps in order to configure IPSec:

1. Configure IKE for Preshared Keys
2. Configure IPSec
3. Configure Network Address Translation (NAT)
4. Configure PIX System Options

Configure IKE for Preshared Keys

Issue the **isakmp enable** command in order to enable IKE on the IPSec terminating interfaces. In this scenario, the outside interface is the IPSec terminating interface on both PIXs. IKE is configured on both PIXs. These commands only show PIX−01.

```
isakmp enable outside
```

You also need to define the IKE policies that are used during the IKE negotiations. Issue the **isakmp policy** command in order to do this. When you issue this command, you must assign a priority level so that the policies are uniquely identified. In this case, the highest priority of 1 is assigned to the policy. The policy is also set to use a preshared key, an MD5 hashing algorithm for data authentication, a DES for Encapsulating Security Payload (ESP), and a Diffie−Hellman group1. The policy is also set to use the SA lifetime.

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

The IKE configuration can be verified with the **show isakmp policy** command:

```
PIX-01#show isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 1000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

Finally, issue the **isakmp key** command in order to configure the preshared key and assign a peer address. The same preshared key must match on the IPSec peers when using preshared keys. The address differs, which depends on the IP address of the remote peer.

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

The policy can be verified with the **write terminal** or **show isakmp** command:

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
```

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

Configure IPSec

IPSec is initiated when one of the PIXs receives traffic that is destined for the other PIX inside network. This traffic is deemed interesting traffic that needs to be protected by IPSec. An access list is used to determine which traffic initiates the IKE and IPSec negotiations. This access list permits traffic to be sent from the 10.1.1.x network, via the IPSec tunnel, to the 172.16.1.x network. The access list on the opposite PIX configuration mirrors this access list. This is appropriate for PIX−01.

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

The IPSec transform set defines the security policy that the peers use to protect the data flow. The IPSec transform is defined by using the **crypto IPSec transform−set** command. A unique name must be chosen for the transform set and up to three transforms can be selected to define the IPSec security protocols. This configuration only uses two transforms: **esp−hmac−md5** and **esp−des**.

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

Crypto maps set up IPSec SAs for the encrypted traffic. You must assign a map name and a sequence number to create a crypto map. Then you define the crypto map parameters. The crypto map transam displayed uses IKE to establish IPSec SAs, encrypts anything that matches access−list 101, has a set peer, and uses the **chevelle** transform−set to enact its security policy for traffic.

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

After you define the crypto map, apply the crypto map to an interface. The interface you choose must be the IPSec terminating interface.

```
crypto map transam interface outside
```

Issue the **show crypto map** command to verify the crypto map attributes.

```
PIX-01#show crypto map

Crypto Map: "transam" interfaces: { outside }

Crypto Map "transam" 1 IPSec-isakmp
Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
Current peer: 172.22.112.12
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ chevelle, }
```

Configure NAT

This command tells the PIX not to NAT any traffic deemed as interesting for IPSec. Thus, all traffic that matches the **access−list** command statements is exempt from the NAT services.

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0
```

```
        nat (inside) 0 access-list NoNAT
```

Configure PIX System Options

Because all inbound sessions must be explicitly permitted by an access list or a conduit, the **sysopt connection permit–IPSec** command is used to permit all inbound IPSec authenticated cipher sessions. With IPSec protected traffic, the secondary conduit check can be redundant and cause the tunnel creation to fail. The **sysopt** command tunes various PIX firewall security and configuration features.

```
        sysopt connection permit-IPSec
```

Configurations

If you have the output of a **write terminal** command from your Cisco device, you can use Output Interpreter ⬏ (registered customers only) to display potential issues and fixes. You must be logged in and have JavaScript enabled to use Output Interpreter ⬏ (registered customers only) .

PIX–01 at 192.68.1.52

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-01
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

!--- Defines interesting traffic that is protected by the IPSec tunnel.


access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- Do not perform NAT for traffic to other PIX Firewall.


access-list NoNAT permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500

!--- Sets the outside address on the PIX Firewall.

```

```
ip address outside 192.168.1.52 255.255.255.0

!--- Sets the inside address on the PIX Firewall.


ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400

!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec.

nat (inside) 0 access-list NoNAT

!--- Sets the default route to the default gateway.

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- Allows IPSec traffic to pass through the PIX Firewall
!--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.

sysopt connection permit-IPSec

!--- IKE Phase 2:
!--- The IPSec transform-set "chevelle" uses esp-md5-hmac to provide
!--- data authentication.


crypto IPSec transform-set chevelle esp-des esp-md5-hmac

!--- Crypto maps set up the SAs for IPSec traffic.
!--- Indicates that IKE is used to establish IPSec SAs.

crypto map transam 1 IPSec-isakmp

!--- Assigns interesting traffic to peer 172.22.112.12.

crypto map transam 1 match address 101

!--- Sets the IPSec peer.
```

```
crypto map transam 1 set peer 172.22.112.12

!--- Sets the IPSec transform set "chevelle"
!--- to be used with the crypto map entry "transam".

crypto map transam 1 set transform-set chevelle

!--- Assigns the crypto map transam to the interface.

crypto map transam interface outside

!--- IKE Phase 1:
!--- Enables IKE on the interface used to terminate the IPSec tunnel

isakmp enable outside

!--- Sets the ISAKMP identity of the peer and
!--- sets the pre-shared key between the IPSec peers.
!--- The same preshared key must be configured on the
!--- IPSec peers for IKE authentication.

isakmp key ******** address 172.22.112.12 netmask 255.255.255.255

!--- The PIX uses the IP address method by default
!--- for the IKE identity in the IKE negotiations.

isakmp identity address

!--- The ISAKMP policy defines the set of parameters
!--- that are used for IKE negotiations.
!--- If these parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the differences in
!--- the default and configured policy.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX−02 at 172.22.112.12

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
```

```
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
```

!--- Defines interesting traffic that is protected by the IPSec tunnel.

access-list 101 permit ip 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0

!--- Do not perform NAT for traffic to other PIX Firewall.

access-list NoNAT permit ip 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0
```
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
```

!--- Sets the outside address on the PIX Firewall.

ip address outside 172.22.112.12 255.255.255.0

!--- Sets the inside address on the PIX Firewall.

ip address inside 172.16.1.1 255.255.255.0
```
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
```

!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec.

nat (inside) 0 access-list NoNAT

!--- Sets the default route to the default gateway.

route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
```

!--- Allows IPSec traffic to pass through the PIX Firewall

```
!--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.

sysopt connection permit-IPSec

!--- IKE Phase 2:
!--- The IPSec transform set defines the negotiated security policy
!--- that the peers use to protect the data flow.
!--- The IPSec transform-set "toyota" uses hmac-md5 authentication header
!--- and encapsulates the payload with des.

crypto IPSec transform-set toyota esp-des esp-md5-hmac

!--- Crypto maps set up the SAs for IPSec traffic.
!--- Indicates that IKE is used to establish IPSec SAs.

crypto map bmw 1 IPSec-isakmp

!--- Assigns interesting traffic to peer 192.168.1.52.

crypto map bmw 1 match address 101

!--- Sets IPSec peer.

crypto map bmw 1 set peer 192.168.1.52

!--- Sets the IPSec transform set "toyota"
!--- to be used with the crypto map entry "bmw".

crypto map bmw 1 set transform-set toyota

!--- Assigns the crypto map bmw to the interface.

crypto map bmw interface outside

!--- IKE Phase 1:
!--- Enables IKE on the interface used to terminate IPSec tunnel.

isakmp enable outside

!--- Sets the ISAKMP identity of the peer and
!--- sets the preshared key between the IPSec peers.
!--- The same preshared key must be configured on the
!--- IPSec peers for IKE authentication.

isakmp key ******** address 192.168.1.52 netmask 255.255.255.255

!--- The PIX uses the IP address method by default
!--- for the IKE identity in the IKE negotiations.

isakmp identity address

!--- The ISAKMP policy defines the set of parameters
!--- that are used for IKE negotiations.
!--- If these parameters are not set, the default parameters are used.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
```

```
: end
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool [⬀] (registered customers only) , which allows you to view an analysis of **show** command output.

- **show crypto IPSec sa** This command displays the current status of the IPSec SAs and is useful in determining if traffic is being encrypted.
- **show crypto isakmp sa** This command shows the current state of the IKE SAs.

PIX–01 show Commands

<table>
<tr><td align="center">PIX–01 show Commands</td></tr>
</table>

```
PIX-01#show crypto IPSec sa
interface: outside
Crypto map tag: transam, local addr. 192.168.1.52

local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 172.22.112.12
PERMIT, flags={origin_is_acl,}

!--- This verifies that encrypted packets are being sent
!--- and received without any errors.

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 192.168.1.52, remote crypto endpt.: 172.22.112.12
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 6f09cbf1

!--- Shows inbound SAs that are established.

inbound esp sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: transam
sa timing: remaining key lifetime (k/sec): (4607999/28430)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

!--- Shows outbound SAs that are established.

outbound ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: transam
```

```
sa timing: remaining key lifetime (k/sec): (4607999/28430)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:




!--- The ISAKMP SA is in the quiescent state (QM_IDLE) when it exists.
!--- The ISAKMP SA is idle. The ISAKMP SA remains authenticated with its
!--- peer and can be used for subsequent Quick Mode exchanges.


PIX-01#show crypto isakmp sa
      dst              src          state       pending        created
172.22.112.12    192.168.1.52     QM_IDLE         0         1Maui-PIX-01#
```

PIX–02 show Commands

```
PIX-02#show crypto IPSec sa

interface: outside
Crypto map tag: bmw, local addr. 172.22.112.12

local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.52
PERMIT, flags={origin_is_acl,}

!--- This verifies that encrypted packets are
!--- being sent and recede without any errors.

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.22.112.12, remote crypto endpt.: 192.168.1.52
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 70be0c04

!--- Shows inbound SAs that are established.

Inbound ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: bmw
sa timing: remaining key lifetime (k/sec): (4607999/28097)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:

!--- Shows outbound SAs that are established.

Outbound ESP sas:
spi: 0x70be0c04(1891503108)
```

```
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: bmw
sa timing: remaining key lifetime (k/sec): (4607999/28097)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:



!--- The ISAKMP SA is in the quiescent state (QM_IDLE) when it exists.
!--- The ISAKMP SA is idle. The ISAKMP SA remains authenticated with its
!--- peer and can be used for subsequent Quick Mode exchanges.

PIX-02#show crypto isakmp sa
    dst              src            state      pending      created
172.22.112.12    192.168.1.52      QM_IDLE        0         PIX-02#
```

The inside interface of the PIX cannot be pinged for the formation of tunnel unless the **management−access** command is configured in the global configuration mode.

```
PIX-02(config)#management−access inside
PIX-02(config)#show management−access
management−access inside
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: The **clear** commands must be performed in configuration mode.

- **clear crypto IPSec sa** This command resets the IPSec SAs after failed attempts to negotiate a VPN tunnel.
- **clear crypto isakmp sa** This command resets the ISAKMP SAs after failed attempts to negotiate a VPN tunnel.

Note: Refer to Important Information on Debug Commands before you issue **debug** commands.

- **debug crypto IPSec** This command shows if a client is negotiating the IPSec portion of the VPN connection.
- **debug crypto isakmp** This command shows if the peers are negotiating the ISAKMP portion of the VPN connection.

After the connection is complete, it can be verified using the **show** commands.

Related Information

- **PIX Support Page**
- **Documentation for PIX Firewall**
- **PIX Command Reference**
- **Request for Comments (RFCs)**

- **IPSec Negotiation/IKE Protocol Support Page**
- **Technical Support & Documentation – Cisco Systems**

Updated: Sep 26, 2008 Document ID: 6211