

Re: Hardware firewall blocking L2TP/IPSec VPN

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.vpn/2007-03/msg00034.html>

- *From:* "Ian" <IanGsi16v@xxxxxxxxxx>
 - *Date:* 14 Mar 2007 09:39:36 -0700
-

Hi Roy,

Thankyou for the informative reply. As you suggested I have been using ike-scan today, I queried the public IP of the VPN server and I received the following information

Enc=3DES, Hash=SHA1, AUTH=PSK, Group=2, Modp=1024, LifeType=Seconds, LifeDuration<4>0x00007080

I received a handshake back.

I then used WireShark to see what was happening when I was trying to connect, from the packets captured it looks as though my clients are trying to authorize using RSA (as I want) while my server is using PSK, I cant seem to work out how to set it to use RSA though.

Below is a export of my wireshark data (public IP removed)

```
No. Time Source Destination
Protocol Info
162 6.206458 192.168.33.66 *public IP* ISAKMP
Identity Protection (Main Mode)
```

```
Frame 162 (354 bytes on wire, 354 bytes captured)
Arrival Time: Mar 14, 2007 16:21:38.625842000
[Time delta from previous packet: 6.206458000 seconds]
[Time since reference or first frame: 6.206458000 seconds]
Frame Number: 162
Packet Length: 354 bytes
Capture Length: 354 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 .... = IG bit: Individual address
```

Re: Hardware firewall blocking L2TP/IPSec VPN

(unicast)
.... .0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... ..0 = IG bit: Individual address
(unicast)
.... .0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ..0 = ECN-CE: 0
Total Length: 340
Identification: 0x19cc (6604)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x348e [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 320
Checksum: 0xd8ad [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
.... ..0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x00000000

Re: Hardware firewall blocking L2TP/IPSec VPN

Length: 312
Security Association payload
Next payload: Vendor ID (13)
Payload length: 200
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
Next payload: NONE (0)
Payload length: 188
Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms: 5
Transform payload # 1
Next payload: Transform (3)
Payload length: 36
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): 2048 bit MODP group (14)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 2
Next payload: Transform (3)
Payload length: 36
Transform number: 2
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 3
Next payload: Transform (3)
Payload length: 36
Transform number: 3
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 4
Next payload: Transform (3)
Payload length: 36

Re: Hardware firewall blocking L2TP/IPSec VPN

Transform number: 4
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 5
Next payload: NONE (0)
Payload length: 36
Transform number: 5
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 24
Vendor ID: MS NT5 ISAKMPOAKLEY
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: Microsoft L2TP/IPSec VPN Client
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Vendor ID payload
Next payload: NONE (0)
Payload length: 20
Vendor ID: unknown vendor ID:
0x26244D38EDDB61B3172A36E3D0CFB819

No. Time Source Destination
Protocol Info
163 6.333779 *public IP* 192.168.33.66 ISAKMP
Informational

Frame 163 (144 bytes on wire, 144 bytes captured)
Arrival Time: Mar 14, 2007 16:21:38.753163000
[Time delta from previous packet: 0.127321000 seconds]
[Time since reference or first frame: 6.333779000 seconds]
Frame Number: 163
Packet Length: 144 bytes
Capture Length: 144 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]

Re: Hardware firewall blocking L2TP/IPSec VPN

[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Dell_2f:cf:d3 (00:14:22:2f:cf:d3), Dst: Intel_aa:
30:b6 (00:11:11:aa:30:b6)
Destination: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... .0. = LG bit: Globally unique
address (factory default)
Source: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... .0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: *public IP* (*public IP*), Dst: 192.168.33.66
(192.168.33.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... .0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 130
Identification: 0xbd15 (48405)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 241
Protocol: UDP (0x11)
Header checksum: 0x2116 [correct]
[Good: True]
[Bad : False]
Source: *public IP* (*public IP*)
Destination: 192.168.33.66 (192.168.33.66)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 110
Checksum: 0xadd1 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 9A261BCCD48A8415
Next payload: Notification (11)

Re: Hardware firewall blocking L2TP/IPSec VPN

Version: 1.0
Exchange type: Informational (5)
Flags: 0x00
.... ..0 = Not encrypted
.... ..0. = No commit
.... ..0.. = No authentication
Message ID: 0x950d9fb2
Length: 102
Notification payload
Next payload: NONE (0)
Payload length: 74
Domain of interpretation: IPSEC (1)
Protocol ID: ISAKMP (1)
SPI Size: 16
Message type: NO-PROPOSAL-CHOSEN (14)
SPI: 0x6569F1BFEE75E44B9A261BCCD48A8415
Notification Data

No. Time Source Destination
Protocol Info
164 7.662331 192.168.33.66 *public IP* ISAKMP
Identity Protection (Main Mode)

Frame 164 (354 bytes on wire, 354 bytes captured)
Arrival Time: Mar 14, 2007 16:21:40.081715000
[Time delta from previous packet: 1.328552000 seconds]
[Time since reference or first frame: 7.662331000 seconds]
Frame Number: 164
Packet Length: 354 bytes
Capture Length: 354 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... ..0 = IG bit: Individual address
(unicast)
.... ..0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... ..0 = IG bit: Individual address
(unicast)
.... ..0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)

Re: Hardware firewall blocking L2TP/IPSec VPN

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 340
Identification: 0x19d1 (6609)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x3489 [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 320
Checksum: 0xd8ad [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
.... ...0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x00000000
Length: 312
Security Association payload
Next payload: Vendor ID (13)
Payload length: 200
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
Next payload: NONE (0)
Payload length: 188
Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0

Re: Hardware firewall blocking L2TP/IPSec VPN

Proposal transforms: 5
Transform payload # 1
Next payload: Transform (3)
Payload length: 36
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): 2048 bit MODP group (14)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 2
Next payload: Transform (3)
Payload length: 36
Transform number: 2
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 3
Next payload: Transform (3)
Payload length: 36
Transform number: 3
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 4
Next payload: Transform (3)
Payload length: 36
Transform number: 4
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 5
Next payload: NONE (0)
Payload length: 36
Transform number: 5

Re: Hardware firewall blocking L2TP/IPSec VPN

Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 24
Vendor ID: MS NT5 ISAKMPOAKLEY
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: Microsoft L2TP/IPSec VPN Client
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Vendor ID payload
Next payload: NONE (0)
Payload length: 20
Vendor ID: unknown vendor ID:
0x26244D38EDDB61B3172A36E3D0CFB819

No. Time Source Destination

Protocol Info

165 7.758516 *public IP* 192.168.33.66 ISAKMP

Informational

Frame 165 (144 bytes on wire, 144 bytes captured)

Arrival Time: Mar 14, 2007 16:21:40.177900000

[Time delta from previous packet: 0.096185000 seconds]

[Time since reference or first frame: 7.758516000 seconds]

Frame Number: 165

Packet Length: 144 bytes

Capture Length: 144 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:udp:isakmp]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: Dell_2f:cf:d3 (00:14:22:2f:cf:d3), Dst: Intel_aa:
30:b6 (00:11:11:aa:30:b6)

Destination: Intel_aa:30:b6 (00:11:11:aa:30:b6)

Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)

.... 0 = IG bit: Individual address
(unicast)

.... 0. = LG bit: Globally unique
address (factory default)

Source: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)

Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)

Re: Hardware firewall blocking L2TP/IPSec VPN

....0 = IG bit: Individual address
(unicast)
....0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: *public IP* (*public IP*), Dst: 192.168.33.66
(192.168.33.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
....0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 130
Identification: 0xcd15 (52501)
Flags: 0x00
0... = Reserved bit: Not set
..0. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 241
Protocol: UDP (0x11)
Header checksum: 0x1116 [correct]
[Good: True]
[Bad : False]
Source: *public IP* (*public IP*)
Destination: 192.168.33.66 (192.168.33.66)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 110
Checksum: 0xadd1 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 9A261BCCD48A8415
Next payload: Notification (11)
Version: 1.0
Exchange type: Informational (5)
Flags: 0x00
....0 = Not encrypted
....0. = No commit
....0.. = No authentication
Message ID: 0x950d9fb2
Length: 102
Notification payload
Next payload: NONE (0)
Payload length: 74
Domain of interpretation: IPSEC (1)

Re: Hardware firewall blocking L2TP/IPSec VPN

Protocol ID: ISAKMP (1)
SPI Size: 16
Message type: NO-PROPOSAL-CHOSEN (14)
SPI: 0x6569F1BFEE75E44B9A261BCCD48A8415
Notification Data

No. Time Source Destination
Protocol Info
166 9.662214 192.168.33.66 *public IP* ISAKMP
Identity Protection (Main Mode)

Frame 166 (354 bytes on wire, 354 bytes captured)
Arrival Time: Mar 14, 2007 16:21:42.081598000
[Time delta from previous packet: 1.903698000 seconds]
[Time since reference or first frame: 9.662214000 seconds]
Frame Number: 166
Packet Length: 354 bytes
Capture Length: 354 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... .0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... .0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... .0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 340
Identification: 0x19d4 (6612)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set

Re: Hardware firewall blocking L2TP/IPSec VPN

..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x3486 [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 320
Checksum: 0xd8ad [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
.... ..0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x00000000
Length: 312
Security Association payload
Next payload: Vendor ID (13)
Payload length: 200
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
Next payload: NONE (0)
Payload length: 188
Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms: 5
Transform payload # 1
Next payload: Transform (3)
Payload length: 36
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): 2048 bit MODP group (14)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)

Re: Hardware firewall blocking L2TP/IPSec VPN

Transform payload # 2
Next payload: Transform (3)
Payload length: 36
Transform number: 2
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 3
Next payload: Transform (3)
Payload length: 36
Transform number: 3
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 4
Next payload: Transform (3)
Payload length: 36
Transform number: 4
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 5
Next payload: NONE (0)
Payload length: 36
Transform number: 5
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 24
Vendor ID: MS NT5 ISAKMPOAKLEY
Vendor ID payload

Re: Hardware firewall blocking L2TP/IPSec VPN

Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: Microsoft L2TP/IPSec VPN Client
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Vendor ID payload
Next payload: NONE (0)
Payload length: 20
Vendor ID: unknown vendor ID:
0x26244D38EDDB61B3172A36E3D0CFB819

No. Time Source Destination
Protocol Info
167 9.738999 *public IP* 192.168.33.66 ISAKMP
Informational

Frame 167 (144 bytes on wire, 144 bytes captured)
Arrival Time: Mar 14, 2007 16:21:42.158383000
[Time delta from previous packet: 0.076785000 seconds]
[Time since reference or first frame: 9.738999000 seconds]
Frame Number: 167
Packet Length: 144 bytes
Capture Length: 144 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Dell_2f:cf:d3 (00:14:22:2f:cf:d3), Dst: Intel_aa:
30:b6 (00:11:11:aa:30:b6)
Destination: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Source: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: *public IP* (*public IP*), Dst: 192.168.33.66
(192.168.33.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)

Re: Hardware firewall blocking L2TP/IPSec VPN

.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 130
Identification: 0x8c11 (35857)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 241
Protocol: UDP (0x11)
Header checksum: 0x521a [correct]
[Good: True]
[Bad : False]
Source: *public IP* (*public IP*)
Destination: 192.168.33.66 (192.168.33.66)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 110
Checksum: 0xadd1 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 9A261BCCD48A8415
Next payload: Notification (11)
Version: 1.0
Exchange type: Informational (5)
Flags: 0x00
.... ...0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x950d9fb2
Length: 102
Notification payload
Next payload: NONE (0)
Payload length: 74
Domain of interpretation: IPSEC (1)
Protocol ID: ISAKMP (1)
SPI Size: 16
Message type: NO-PROPOSAL-CHOSEN (14)
SPI: 0x6569F1BFEE75E44B9A261BCCD48A8415
Notification Data

No. Time Source Destination
Protocol Info
180 13.661940 192.168.33.66 *public IP* ISAKMP
Identity Protection (Main Mode)

Frame 180 (354 bytes on wire, 354 bytes captured)

Re: Hardware firewall blocking L2TP/IPSec VPN

Re: Hardware firewall blocking L2TP/IPSec VPN

Arrival Time: Mar 14, 2007 16:21:46.081324000
[Time delta from previous packet: 3.922941000 seconds]
[Time since reference or first frame: 13.661940000 seconds]
Frame Number: 180
Packet Length: 354 bytes
Capture Length: 354 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... 0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 340
Identification: 0x19da (6618)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x3480 [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)

Re: Hardware firewall blocking L2TP/IPSec VPN

Length: 320
Checksum: 0xd8ad [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
.... ..0 = Not encrypted
.... ..0. = No commit
.... ..0.. = No authentication
Message ID: 0x00000000
Length: 312
Security Association payload
Next payload: Vendor ID (13)
Payload length: 200
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
Next payload: NONE (0)
Payload length: 188
Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms: 5
Transform payload # 1
Next payload: Transform (3)
Payload length: 36
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): 2048 bit MODP group (14)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 2
Next payload: Transform (3)
Payload length: 36
Transform number: 2
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)

Re: Hardware firewall blocking L2TP/IPSec VPN

Transform payload # 3
Next payload: Transform (3)
Payload length: 36
Transform number: 3
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Alternate 1024-bit MODP group
(2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 4
Next payload: Transform (3)
Payload length: 36
Transform number: 4
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 5
Next payload: NONE (0)
Payload length: 36
Transform number: 5
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 24
Vendor ID: MS NT5 ISAKMPOAKLEY
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: Microsoft L2TP/IPSec VPN Client
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Vendor ID payload
Next payload: NONE (0)
Payload length: 20
Vendor ID: unknown vendor ID:
0x26244D38EDDB61B3172A36E3D0CFB819

Re: Hardware firewall blocking L2TP/IPSec VPN

No. Time Source Destination
Protocol Info
181 13.749030 *public IP* 192.168.33.66 ISAKMP
Informational

Frame 181 (144 bytes on wire, 144 bytes captured)
Arrival Time: Mar 14, 2007 16:21:46.168414000
[Time delta from previous packet: 0.087090000 seconds]
[Time since reference or first frame: 13.749030000 seconds]
Frame Number: 181
Packet Length: 144 bytes
Capture Length: 144 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Dell_2f:cf:d3 (00:14:22:2f:cf:d3), Dst: Intel_aa:
30:b6 (00:11:11:aa:30:b6)
Destination: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Source: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: *public IP* (*public IP*), Dst: 192.168.33.66
(192.168.33.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... 0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 130
Identification: 0xc614 (50708)
Flags: 0x00
0... = Reserved bit: Not set
..0. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 241
Protocol: UDP (0x11)
Header checksum: 0x1817 [correct]

Re: Hardware firewall blocking L2TP/IPSec VPN

[Good: True]
[Bad : False]
Source: *public IP* (*public IP*)
Destination: 192.168.33.66 (192.168.33.66)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 110
Checksum: 0xadd1 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 9A261BCCD48A8415
Next payload: Notification (11)
Version: 1.0
Exchange type: Informational (5)
Flags: 0x00
.... ..0 = Not encrypted
.... ..0. = No commit
.... ..0.. = No authentication
Message ID: 0x950d9fb2
Length: 102
Notification payload
Next payload: NONE (0)
Payload length: 74
Domain of interpretation: IPSEC (1)
Protocol ID: ISAKMP (1)
SPI Size: 16
Message type: NO-PROPOSAL-CHOSEN (14)
SPI: 0x6569F1BFEE75E44B9A261BCCD48A8415
Notification Data

No. Time Source Destination
Protocol Info
188 21.661417 192.168.33.66 *public IP* ISAKMP
Identity Protection (Main Mode)

Frame 188 (354 bytes on wire, 354 bytes captured)
Arrival Time: Mar 14, 2007 16:21:54.080801000
[Time delta from previous packet: 7.912387000 seconds]
[Time since reference or first frame: 21.661417000 seconds]
Frame Number: 188
Packet Length: 354 bytes
Capture Length: 354 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)

Re: Hardware firewall blocking L2TP/IPSec VPN

Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... 0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 340
Identification: 0x19db (6619)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x347f [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 320
Checksum: 0xd8ad [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
.... 0 = Not encrypted

Re: Hardware firewall blocking L2TP/IPSec VPN

.... .0. = No commit
.... .0.. = No authentication
Message ID: 0x00000000
Length: 312
Security Association payload
Next payload: Vendor ID (13)
Payload length: 200
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
Next payload: NONE (0)
Payload length: 188
Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms: 5
Transform payload # 1
Next payload: Transform (3)
Payload length: 36
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): 2048 bit MODP group (14)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 2
Next payload: Transform (3)
Payload length: 36
Transform number: 2
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 3
Next payload: Transform (3)
Payload length: 36
Transform number: 3
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)

Re: Hardware firewall blocking L2TP/IPSec VPN

Transform payload # 4
Next payload: Transform (3)
Payload length: 36
Transform number: 4
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 5
Next payload: NONE (0)
Payload length: 36
Transform number: 5
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 24
Vendor ID: MS NT5 ISAKMPOAKLEY
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: Microsoft L2TP/IPSec VPN Client
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Vendor ID payload
Next payload: NONE (0)
Payload length: 20
Vendor ID: unknown vendor ID:
0x26244D38EDDB61B3172A36E3D0CFB819

No. Time Source Destination
Protocol Info
189 21.781681 *public IP* 192.168.33.66 ISAKMP
Informational

Frame 189 (144 bytes on wire, 144 bytes captured)
Arrival Time: Mar 14, 2007 16:21:54.201065000
[Time delta from previous packet: 0.120264000 seconds]
[Time since reference or first frame: 21.781681000 seconds]
Frame Number: 189
Packet Length: 144 bytes

Re: Hardware firewall blocking L2TP/IPSec VPN

Capture Length: 144 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Dell_2f:cf:d3 (00:14:22:2f:cf:d3), Dst: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Destination: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address (unicast)
... 0. = LG bit: Globally unique address (factory default)
Source: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address (unicast)
... 0. = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: *public IP* (*public IP*), Dst: 192.168.33.66 (192.168.33.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... 0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 130
Identification: 0xab14 (43796)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 241
Protocol: UDP (0x11)
Header checksum: 0x3317 [correct]
[Good: True]
[Bad : False]
Source: *public IP* (*public IP*)
Destination: 192.168.33.66 (192.168.33.66)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 110
Checksum: 0xadd1 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol

Re: Hardware firewall blocking L2TP/IPSec VPN

Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 9A261BCCD48A8415
Next payload: Notification (11)
Version: 1.0
Exchange type: Informational (5)
Flags: 0x00
.... ...0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x950d9fb2
Length: 102
Notification payload
Next payload: NONE (0)
Payload length: 74
Domain of interpretation: IPSEC (1)
Protocol ID: ISAKMP (1)
SPI Size: 16
Message type: NO-PROPOSAL-CHOSEN (14)
SPI: 0x6569F1BFEE75E44B9A261BCCD48A8415
Notification Data

No. Time Source Destination
Protocol Info
207 37.676004 192.168.33.66 *public IP* ISAKMP
Identity Protection (Main Mode)

Frame 207 (354 bytes on wire, 354 bytes captured)
Arrival Time: Mar 14, 2007 16:22:10.095388000
[Time delta from previous packet: 15.894323000 seconds]
[Time since reference or first frame: 37.676004000 seconds]
Frame Number: 207
Packet Length: 354 bytes
Capture Length: 354 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... ...0 = IG bit: Individual address
(unicast)
.... ..0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... ...0 = IG bit: Individual address
(unicast)
.... ..0. = LG bit: Globally unique
address (factory default)

Re: Hardware firewall blocking L2TP/IPSec VPN

Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 340
Identification: 0x19dd (6621)
Flags: 0x00
0... = Reserved bit: Not set
..0. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x347d [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 320
Checksum: 0xd8ad [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
.... ...0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x00000000
Length: 312
Security Association payload
Next payload: Vendor ID (13)
Payload length: 200
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
Next payload: NONE (0)
Payload length: 188

Re: Hardware firewall blocking L2TP/IPSec VPN

Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms: 5
Transform payload # 1
Next payload: Transform (3)
Payload length: 36
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): 2048 bit MODP group (14)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 2
Next payload: Transform (3)
Payload length: 36
Transform number: 2
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 3
Next payload: Transform (3)
Payload length: 36
Transform number: 3
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): 3DES-CBC (5)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 4
Next payload: Transform (3)
Payload length: 36
Transform number: 4
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Transform payload # 5

Re: Hardware firewall blocking L2TP/IPSec VPN

Next payload: NONE (0)
Payload length: 36
Transform number: 5
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): DES-CBC (1)
Hash-Algorithm (2): MD5 (1)
Group-Description (4): Default 768-bit MODP group (1)
Authentication-Method (3): RSA-SIG (3)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 24
Vendor ID: MS NT5 ISAKMPOAKLEY
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: Microsoft L2TP/IPSec VPN Client
Vendor ID payload
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Vendor ID payload
Next payload: NONE (0)
Payload length: 20
Vendor ID: unknown vendor ID:
0x26244D38EDDB61B3172A36E3D0CFB819

No. Time Source Destination
Protocol Info
208 37.791529 *public IP* 192.168.33.66 ISAKMP
Informational

Frame 208 (144 bytes on wire, 144 bytes captured)
Arrival Time: Mar 14, 2007 16:22:10.210913000
[Time delta from previous packet: 0.115525000 seconds]
[Time since reference or first frame: 37.791529000 seconds]
Frame Number: 208
Packet Length: 144 bytes
Capture Length: 144 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Dell_2f:cf:d3 (00:14:22:2f:cf:d3), Dst: Intel_aa:
30:b6 (00:11:11:aa:30:b6)
Destination: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique

Re: Hardware firewall blocking L2TP/IPSec VPN

address (factory default)
Source: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... ..0 = IG bit: Individual address
(unicast)
.... ..0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: *public IP* (*public IP*), Dst: 192.168.33.66
(192.168.33.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ..0 = ECN-CE: 0
Total Length: 130
Identification: 0x3610 (13840)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 241
Protocol: UDP (0x11)
Header checksum: 0xa81b [correct]
[Good: True]
[Bad : False]
Source: *public IP* (*public IP*)
Destination: 192.168.33.66 (192.168.33.66)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 110
Checksum: 0xadd1 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Security Association and Key Management Protocol
Initiator cookie: 6569F1BFEE75E44B
Responder cookie: 9A261BCCD48A8415
Next payload: Notification (11)
Version: 1.0
Exchange type: Informational (5)
Flags: 0x00
.... ..0 = Not encrypted
.... ..0. = No commit
.... .0.. = No authentication
Message ID: 0x950d9fb2
Length: 102
Notification payload

Re: Hardware firewall blocking L2TP/IPSec VPN

Next payload: NONE (0)
Payload length: 74
Domain of interpretation: IPSEC (1)
Protocol ID: ISAKMP (1)
SPI Size: 16
Message type: NO-PROPOSAL-CHOSEN (14)
SPI: 0x6569F1BFEE75E44B9A261BCCD48A8415
Notification Data

No. Time Source Destination
Protocol Info
242 69.728963 192.168.33.66 *public IP* ISAKMP
Informational

Frame 242 (98 bytes on wire, 98 bytes captured)
Arrival Time: Mar 14, 2007 16:22:42.148347000
[Time delta from previous packet: 31.937434000 seconds]
[Time since reference or first frame: 69.728963000 seconds]
Frame Number: 242
Packet Length: 98 bytes
Capture Length: 98 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:isakmp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_aa:30:b6 (00:11:11:aa:30:b6), Dst:
Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Destination: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
Address: Dell_2f:cf:d3 (00:14:22:2f:cf:d3)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Source: Intel_aa:30:b6 (00:11:11:aa:30:b6)
Address: Intel_aa:30:b6 (00:11:11:aa:30:b6)
.... 0 = IG bit: Individual address
(unicast)
.... 0. = LG bit: Globally unique
address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.33.66 (192.168.33.66), Dst: *public
IP* (*public IP*)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
0000 00. = Differentiated Services Codepoint: Default (0x00)
.... 0. = ECN-Capable Transport (ECT): 0
.... 0 = ECN-CE: 0
Total Length: 84
Identification: 0x19de (6622)

Re: Hardware firewall blocking L2TP/IPSec VPN

Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x357c [correct]
[Good: True]
[Bad : False]
Source: 192.168.33.66 (192.168.33.66)
Destination: *public IP* (*public IP*)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port: isakmp (500)
Length: 64
Checksum: 0xcbd0 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Internet Securit