

test_capture2.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

icmp

No.	Time	Source	Destination	Protocol	Length	Info
10844	11.814441	192.168.2.151	192.168.2.1	ICMP	282	Destination unreachable (Port unreachable)

> Frame 10844: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits)

> Ethernet II, Src: AzureWaveTec_8c:87:eb (14:13:33:8c:87:eb), Dst: TendaTechnol_15:67:e0 (d8:32:14:15:67:e0)

> Destination: TendaTechnol_15:67:e0 (d8:32:14:15:67:e0)

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

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

> Source: AzureWaveTec_8c:87:eb (14:13:33:8c:87:eb)

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

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

Type: IPv4 (0x0800)

[Stream index: 0]

> Internet Protocol Version 4, Src: 192.168.2.151, Dst: 192.168.2.1> Internet Control Message Protocol

0000 d8 32 14 15 67 e0 14 13 33 8c 87 eb 08 00 45 00 .2.g... 3....E.

0010 01 0c cb ea 00 00 80 01 e8 1d c0 a8 02 97 c0 a8E....J

0020 02 01 03 03 83 d3 00 00 00 00 45 00 00 f0 a3 4aE....J

0030 40 00 40 11 10 ca c0 a8 02 01 c0 a8 02 97 00 35 @.@.....5

0040 e3 a1 00 dc 91 83 da ac 81 80 00 01 00 02 00 015

0050 00 00 05 74 65 61 6d 73 06 65 76 65 6e 74 73 04 ...teams events-

0060 64 61 74 61 09 6d 69 63 72 6f 73 6f 66 74 03 63 data-microsoft-c

0070 6f 6d 00 00 41 00 01 c0 0c 00 05 00 01 00 00 00 om.A.....

0080 6b 00 26 11 74 65 61 6d 73 2d 65 76 65 6e 74 73 k.&team s-events

0090 2d 64 61 74 61 0e 74 72 61 66 66 69 63 6d 61 6e -data trafficman

00a0 61 67 65 72 03 6e 65 74 00 c0 3d 00 05 00 01 00 ager.net ..=.....

00b0 00 00 3c 00 29 10 6f 6e 65 64 73 63 6f 6c 70 72 ..<.)on edscolpr

00c0 64 77 75 73 32 30 06 77 65 73 74 75 73 08 63 6c dwus20.w estus-cl

00d0 6f 75 64 61 70 70 05 61 7a 75 72 65 c0 28 c0 80 oudapp-a zure-(..

00e0 00 06 00 01 00 00 00 3c 00 30 06 6e 73 31 2d 30< -0-ns1-0

00f0 32 09 61 7a 75 72 65 2d 64 6e 73 c0 28 06 6d 73 2-azure- dns-(ms

0100 6e 68 73 74 c0 1e 00 00 27 11 00 00 03 84 00 00 nhst.....'

0110 01 2c 00 09 3a 80 00 00 00 3c ,...<

```
C:\Windows\System32>ping www.youtube.com
```

```
Pinging youtube-ui.l.google.com [142.250.192.14] with 32 bytes of data:
```

```
Reply from 142.250.192.14: bytes=32 time=30ms TTL=111
```

```
Reply from 142.250.192.14: bytes=32 time=29ms TTL=111
```

```
Reply from 142.250.192.14: bytes=32 time=30ms TTL=111
```

```
Reply from 142.250.192.14: bytes=32 time=32ms TTL=111
```

```
Ping statistics for 142.250.192.14:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 29ms, Maximum = 32ms, Average = 30ms
```


test_capture2.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

tls

No.	Time	Source	Destination	Protocol	Length	Info
7895	8.471871	192.168.2.191	192.168.2.151	TLSv1.2	403	Application Data
7903	8.474090	192.168.2.151	192.168.2.191	TLSv1.2	318	Application Data
10166	11.132308	192.168.2.151	48.218.107.40	TLSv1.2	104	Application Data
10317	11.282903	48.218.107.40	192.168.2.151	TLSv1.2	93	Application Data
11036	12.059449	192.168.2.151	20.189.173.25	TLSv1.3	482	Client Hello (SNI=teams.events.data.microsoft.com)
11338	12.301128	192.168.2.151	20.189.173.25	TLSv1.3	514	Client Hello (SNI=teams.events.data.microsoft.com)
11370	12.313095	20.189.173.25	192.168.2.151	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
11390	12.318607	192.168.2.151	20.189.173.25	TLSv1.3	768	Change Cipher Spec, Client Hello (SNI=teams.events.data.microsoft.com)
11539	12.566876	20.189.173.25	192.168.2.151	TLSv1.3	1514	Server Hello
11544	12.567970	20.189.173.25	192.168.2.151	TLSv1.3	620	Application Data
11550	12.570278	192.168.2.151	20.189.173.25	TLSv1.3	128	Application Data
11552	12.571274	192.168.2.151	20.189.173.25	TLSv1.3	146	Application Data

> Frame 7895: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits)

> Ethernet II, Src: c2:76:87:74:e6:22 (c2:76:87:74:e6:22), Dst: AzureWaveTec_8c:87:eb (14:13:33:8c:87:eb)

> Destination: AzureWaveTec_8c:87:eb (14:13:33:8c:87:eb)

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

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

> Source: c2:76:87:74:e6:22 (c2:76:87:74:e6:22)

.....1. = LG bit: Locally administered address (this is NOT the default)

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

Type: IPv4 (0x0800)

[Stream index: 7]

> Internet Protocol Version 4, Src: 192.168.2.191, Dst: 192.168.2.151

> Transmission Control Protocol, Src Port: 52370, Dst Port: 53289, Seq: 1, Ack: 1, Len: 349

> Transport Layer Security

00001413338c87ebc2768774e62208004500...3...v-t..."E-00100185000040004006b2cc0a802bf0a8...@_@...00200297cc92d0294cad0b93174a8a475018...L...J.GP-00301000e9dc000017030301583fc9e23aa5...X?...0040e187bbf38afe3bb404bf68c21ec6abd3...;...h...0050baecaf7fe8febb454aee8bc1092d3e1e...EJ...->006033628133957bec198808b635405bca043b33...5@[...007012b2a0a2553f71c312edb6f693eda0d7...U?q...00805e91a847ce13e5ef8a2756f6f7a864b2...G...V...d-0090ae3fb7571a0a46dd93b63ed9837929cd...?W...F...>y).00a09c80798fc553d59a023cea6a01e6231e...y...S...<j...#-00b0340a77db9028125104f7bbca0bb7af32c4-w...(-Q...z-,Yj...f...d*...00c0596a00dd186601c488860b647f2ab7f6...@4...2...Vk...00d0be40342ee232e595f4f29c06566baf02f...@...qk...8M...00e066802c9a40cca6716b0ae10407384d17f...7...oa...=|...00f0221fc63701a16f6102cb06943d0b7c94...d...;3...ZNK...01001f64b4be0fe3b113399125a4e4ba1f80e...O...<...R...(-D_T01105f4f19803cfa949c5286aa288a445f54N;...*P...01204e3bb0f3dde92a5011d207889df7e3e4...^ne...0y...N)...0130ffbb5e6e65c59f0d307981d44e5d48e...i...+...g...01401ba069f3c82b912e95a3c9b9f6d467ddFKY...6...s*...0150464b5981a6a69f93848f36ac732a0eb2AK+...??...0160414b2b1a06eb7e8291143f85d91a3a98...#...}...dp-at01700a2384d7edc6d97d4a00e6470ca6174...h...9<H...}01800f7e68c086393c9948ba0b0b1caeda17d...a019082ed61

Rule Type

Select the type of firewall rule to create.

- Steps:
- Rule Type
 - Protocol and Ports
 - Action
 - Profile
 - Name

What type of rule would you like to create?

- ☐ **Program**
Rule that controls connections for a program.
- ☒ **Port**
Rule that controls connections for a TCP or UDP port.
- ☐ **Predefined:**

AllJoyn Router

Rule that controls connections for a Windows experience.
- ☐ **Custom**
Custom rule.

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

- ☒ TCP
- ☐ UDP

Does this rule apply to all local ports or specific local ports?

- ☐ All local ports
- ☒ Specific local ports:

23

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Customize...

☒ **Block the connection**

< Back

Next >

Cancel

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

When does this rule apply?

☒ **Domain**

Applies when a computer is connected to its corporate domain.

☒ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**

Applies when a computer is connected to a public network location.

< Back

Next >

Cancel

Windows Defender Firewall with

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Inbound Rules

Name

test2

✓

Aimlabs

✓

Aimlabs

✓

AnyDesk

✓

AnyDesk

✓

AnyDesk

✓

AnyDesk

✓

AnyDesk

✓

AnyDesk

✓

anydesk.exe

✓

anydesk.exe

✓

BitTorrent (TCP-In)

✓

BitTorrent (UDP-In)

✓

BlueStacks Service

✓

BlueStacksWeb

✓

Bonjour Service

✓

Bonjour Service

✓

Bonjour Service

✓

Bonjour Service

✓

Cloud Game

✓

Deceit

✓

Deceit

✓

EpicWebHelper

✓

EpicWebHelper

Actions

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

test2

Disable Rule

Cut

Copy

Delete

Properties

Help

Domain network

Networks at a workplace that are joined to a domain.

Active domain networks

Not connected

Quick Heal Firewall

Quick Heal Firewall is turned on.

 No action needed.

[Open app](#)

Microsoft Defender Firewall

Microsoft Defender Firewall is not active, because you're using other providers.