



External communication

- [External communication, on page 1](#)

External communication

An external communication is a communication initiated between a component/device inside a monitored network and an external component/device.







External communications are stored and listed in Cisco Cyber Vision, but not the external components/devices, nor their flows, to not obstruct the system. As a result, Cisco Cyber Vision's performances are increased, the GUI is cleared from unnecessary data, and the license device count and risk scores are limited to inner devices and more accurate.

By default, external communications are defined as such through the detection of external components' IP addresses that **do not** meet with private IP address formats.

IP addresses that meet with private formats are considered as internal by default and are processed under stored components or devices and are displayed in Cisco Cyber Vision.

However, because sometimes public IP addresses are used in a private network of an industrial site, it is possible to manually define communications by declaring IP ranges as internal or external through the Network Organization administration page. For more information, refer to Cisco Cyber Vision GUI Administration Guide.

It is also possible to declare as external all or part of a private subnetwork. For example to filter some IT components/devices which are not relevant for Cisco Cyber Vision.

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
<input type="checkbox"/> 10.0.0/8		10/8 private network	External	 
10.2.0/22		OT range	OT Internal	 
10.4.0/22		External IP within IP range	IT Internal	 

In the GUI, a component with external communications is shown as an icon bordered in orange, or a double orange border for a device.

A device with external communications in the Map:

The screenshot displays a network management interface. On the left, a legend defines traffic content (Important, Control system behavior, IT Behavior, Security analysis, Network analysis, Others) and traffic type (Conduit, Point to point). Below the legend, options include 'Show network activities'. The main area shows a network diagram with a central 'vmware' device (IP: 10.2.2.62) highlighted with an orange border. Other devices include '310ER/A', '224.0.0.25', '10.2.3.251', '224.0.0.2', and 'LLDP Multicast'. On the right, a detailed view for the 'vmware' device (IP: 10.2.2.62) is shown. It includes a 'Device with external communications' button with a globe icon and the number '12'. Below this, the device's technical sheet is displayed, showing activity tags (Time Management, Low Volume, Multicast), activity tags (ARP, DNS, NTP, SMB, SSL/TLS), a risk score of 35, and various properties (ip, mac, name, public-ip, vendor-name).

If you click on this component, its right side panel will appear. The **External Communications** button with the number of external communications will open the component's technical sheet directly on the external communications list.

*The device's right side panel and the **External Communications** button:*

Device with external communications

Sensors: -

Tags: DNS Server, HTTP Client, HTTPS Client

Activity tags: Time Management, Low Volume, Multicast, ARP, DNS, NTP, SMB, SSL/TLS

Risk score: 35 [See details](#)

Components: 10.2.2.62

Properties: ip: 10.2.2.62
mac: 00:50:56:8f:10:eb
name: 10.2.2.62
public-ip: no
vendor-name: VMware, Inc.
[... show more](#)

Custom Properties: [+ Add properties](#)

Summary Dashboard:

- Activities: 9
- Events: 2
- Vulnerability: 0
- Credential: 0
- Variable: 0
- External Comm.: 31

The external communications list in the device's technical sheet:

31 External Communications [Export to CSV](#)

[All](#) [Inbound](#) [Outbound](#) < 1 2 > 20 / page v

Source IP	Destination IP	Destination Port	Hostname	Protocol	Received by device	Sent by device	Last Seen	Direction
10.2.2.62	142.250.179.142	443	www.youtube.com	HTTPS	31.3 kB	1.17 MB	23 days ago	Outbound
10.2.2.62	192.229.221.95	80	ocsp.digicert.com	HTTP	709 B	982 B	23 days ago	Outbound
10.2.2.62	92.123.77.17	80	r3.o.lencr.org	HTTP	3.32 kB	6.03 kB	23 days ago	Outbound
10.2.2.62	18.239.100.55	80	ocsp.r2m02.amazontrust.com	HTTP	718 B	1.19 kB	23 days ago	Outbound
10.2.2.62	34.107.221.82	80	detectportal.firefox.com	HTTP	586 B	544 B	23 days ago	Outbound

The list shows details about external communications such as source and destination IPs, destination port, hostname, protocol, whether they are inbound or outbound, etc.

It is possible to export this list using the **Export to CSV** button.

