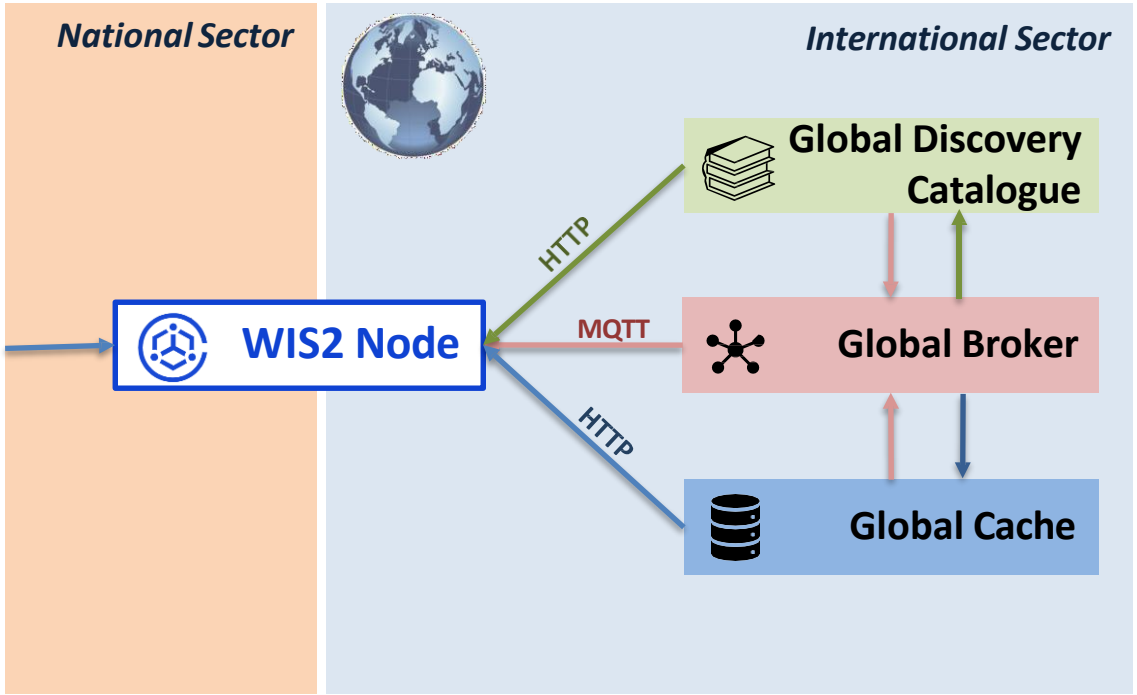
WIS2 Node implementation: networking, security and maintenance

Reminder: what is a WIS2 Node ?

The WIS2 node is composed of 2 endpoints that need to be exposed over the public Internet:

- MQTT broker: to publish WIS2 notifications for metadata and data
- HTTP endpoint: to enable the download of data files and metadata records



Security recommendations:

- Only open ports for HTTP and MQTT to external connections
- Read-only access to HTTP and MQTT
- Encrypt HTTP and MQTT using TLS
- Use firewall limit access to trusted incoming connections (Global Services and local partners)

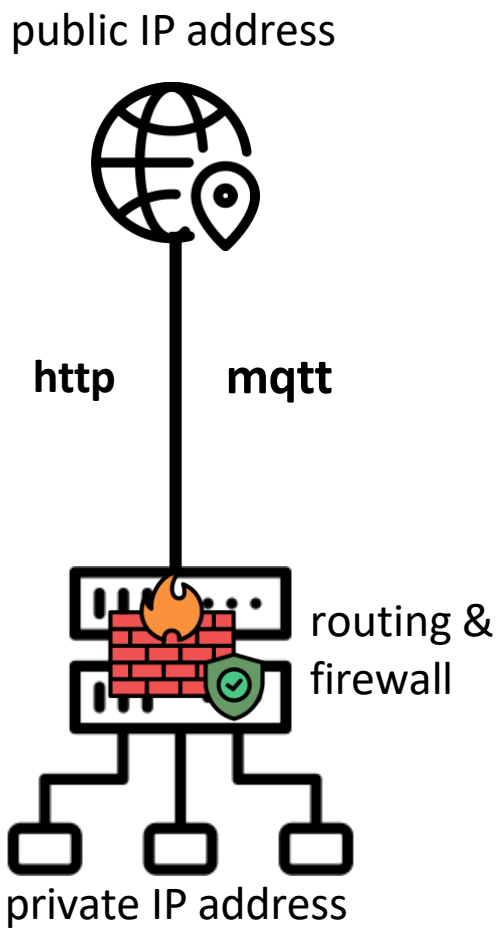
Network and security

Traffic of your WIS2 node needs to be routed to a public IP address

Incoming connections limited to MQTT and HTTP ports

Cloud: use cloud interface to request a public IP address and manage the allowed incoming connections via security groups

On-premise: work with local IT/Network Team to provide public IP address and manage routing and firewall



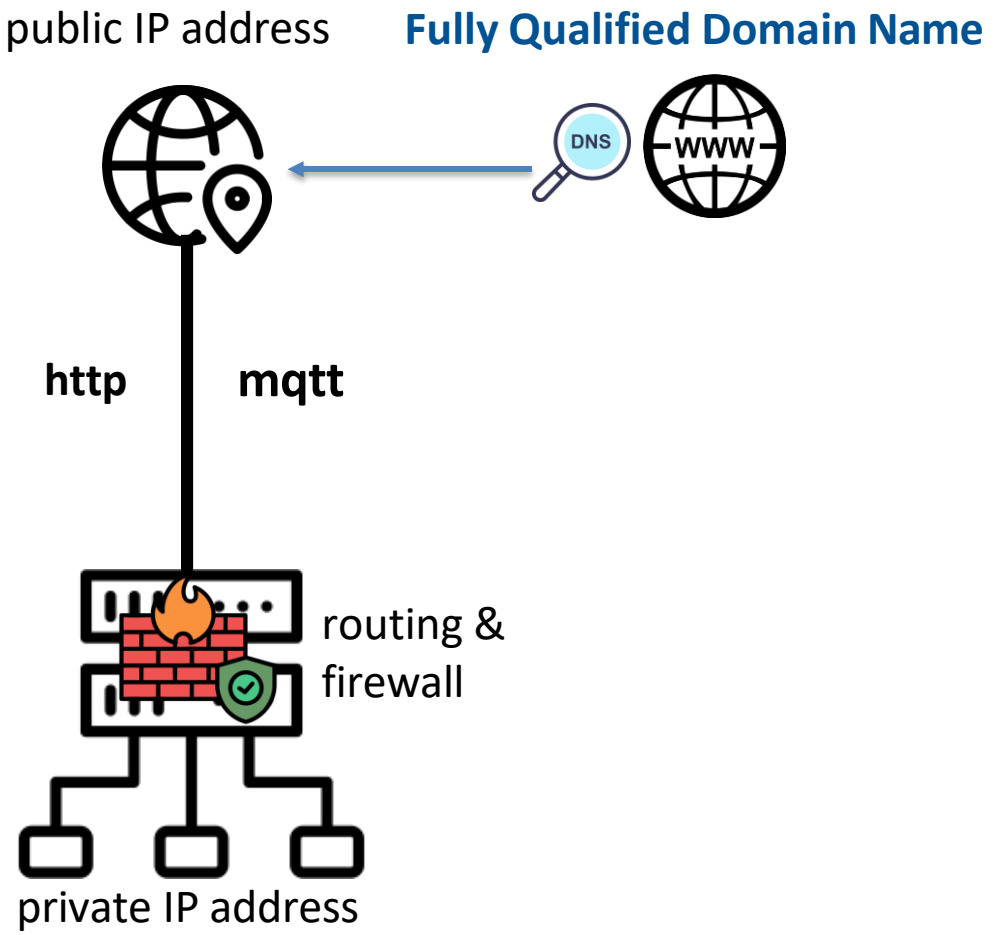
Setting up a web address for your WIS2 Node

An FQDN (Fully Qualified Domain Name) specifies the **web address** for your WIS2 Node

Coordinate with your IT/Network Team:

- Choose a specific subdomain for your WIS2 node on your organization primary domain:
  e.g: *wis2node.wis.cma.cn*

- Request to create a DNS record pointing the subdomain to the public IP address of your WIS2 Node



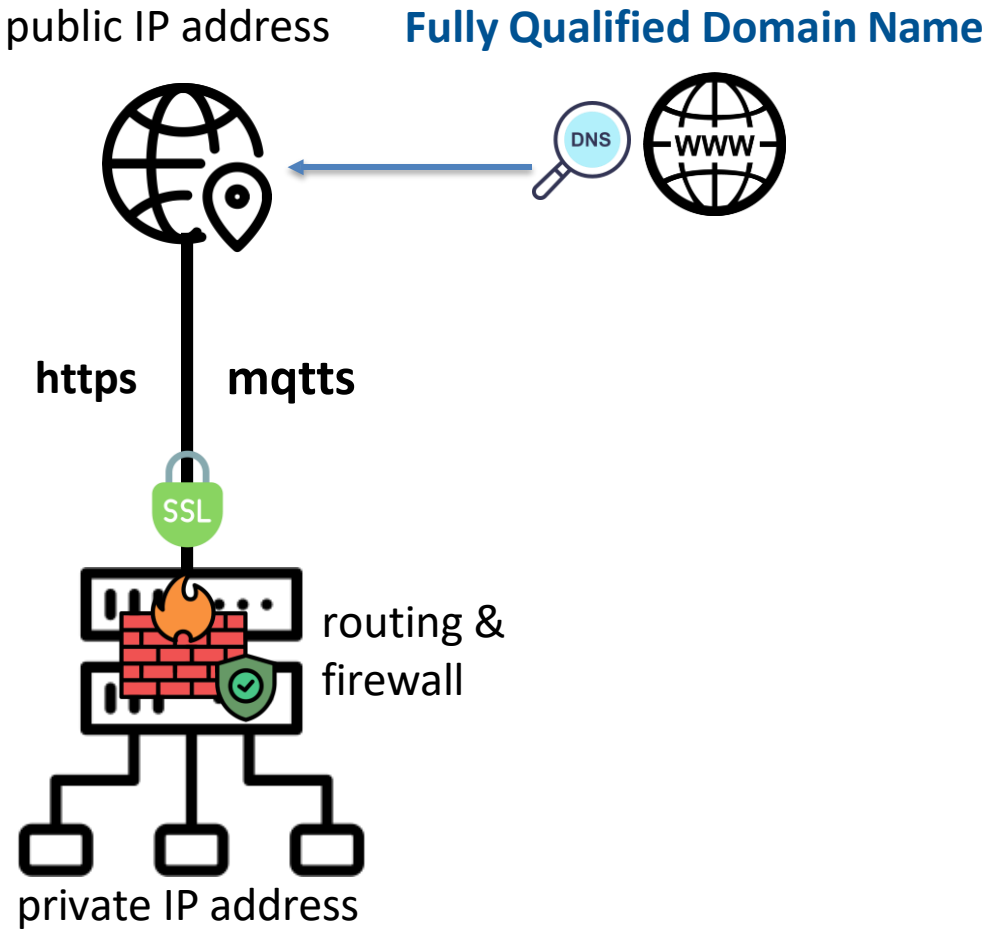
TLS/SSL Certificates for HTTP and MQTT encryption

Use TLS/SSL certificates to encrypt your data and ensure clients can validate the identify of your host

Purchase an TLS/SSL certificates from a trusted Certificate Authority (CA) or use a free CA like *Let's Encrypt*

TLS/SSL certificates can be installed in a proxy routing the HTTP traffic from your wis2box-host to the public Internet

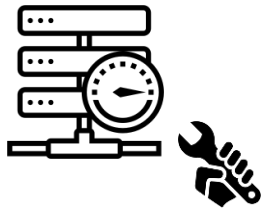
wis2box can use TLS/SSL certificates installed in your host (see wis2box documentation)



WORLD METEOROLOGICAL ORGANIZATION

1950-2025 SCIENCE for ACTION

WIS2 Node Operations: Maintenance and monitoring

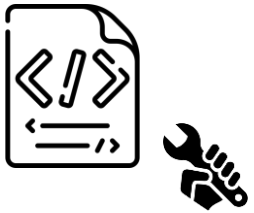


Host monitoring:

- Uptime
- Internet access
- CPU and memory
- Disk usage

Software updates:

- WIS2 Node software (e.g. wis2box, IBL MW …)
- host operating system
- any other software dependencies



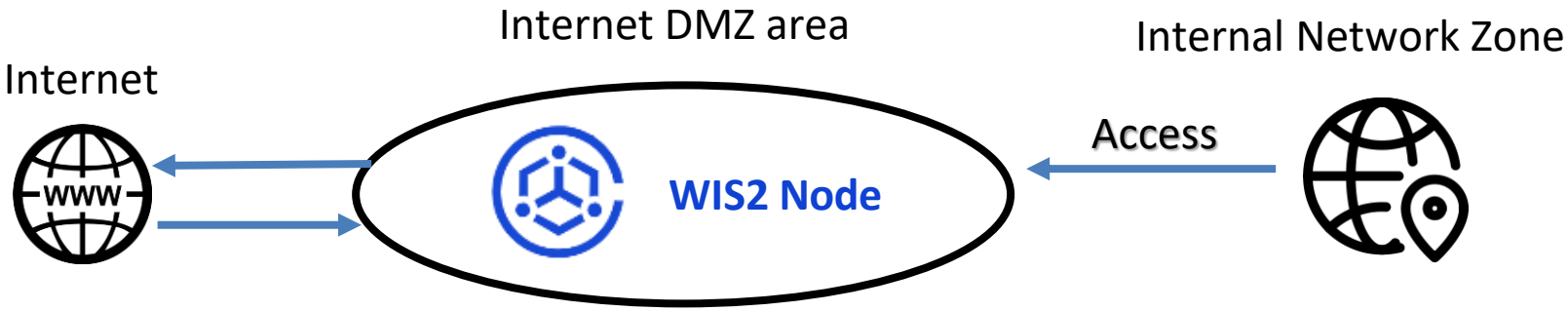
WIS2 Node configuration updates:

- Datasets and associated discovery metadata
- Station list and associated WIGOS station metadata
- Regularly review data quality of published data

WIS2 Node Implementation: GISC Beijing

Encryption for HTTP and MQTT: Purchase an SSL certificate from a trusted Certificate Authority (CA).

- http → https
- mqtt 1883 (normal TCP connection) → mqtts 8883 (safe connection based on SSL)



System monitoring: 1) local monitoring system of CMA(alert). 2)GM dashboard (routine check). 3) Subscribe to the topic of `monitor` to get the alerts. (in developing) 4. Jira tickets on IMS (routine check).

Hardware monitoring: Dedicated divisions responsible for maintaining the servers, network and operating system.

Software update: Follows the GitHub update of wis2box.

METEOROLOGICAL ORGANIZATION | SCIENCE for ACTION

Thank you
Merci
Gracias
كل ارًكش
谢谢
Спасибо