IXON Cloud Security Whitepaper

Ensuring a safe, reliable and trustworthy IIoT solution

www.ixon.cloud →

Table of contents

Introduction

IXON provides a fully integrated cloud-based Industrial IoT solution.

IXON provides a fully integrated cloud-based Industrial IoT solution for machine builders, building automation integrators and system integrators. The IXON Cloud platform together with a connectivity gateway, the IXrouter or third party devices with the IXagent software installed, offers an all-in-one solution for safely and easily setting up remote access to your machines, monitoring or logging machine status and receiving alerts about important machine events — all within your own branded IXON Cloud portal.

As a cloud solution provider, IXON fully understands the security implications of operating in the cloud. All products and services are designed to provide better security than many traditional on-premise solutions.

Security shapes the day-to-day business of IXON, how they develop products, design the IXON Cloud infrastructure, and more. This paper outlines IXON's approach to security for the IXON Cloud platform and the associated IXrouter. IXON's security strategy is based on the CIA triad: a security management model for protecting the confidentiality, integrity and availability of information.

Over 1.000 companies worldwide have already chosen the IXON Cloud solution. With over 10.000 IXON Cloud platform users, the IXON Cloud continues to grow rapidly and it is imperative to keep all data secure — following industry best practices.

> "Data protection is IXON's number one priority and the cornerstone of everyday operations."

“Machine builders entrust us with critical data and it is our number one priority to protect this data at all costs, and make sure that it's always available. We created an ISO 27001 based security management (ISMS) in order to identify, prevent and defend against any vulnerabilities that may arise. This systematic approach allows us to achieve our main goals: no security incidents, maximal uptime and no data loss.

Willem Hofmans, CEO at IXON

Information security management

Protecting the confidentiality, availability and integrity of all data

A better world starts with yourself. IXON believes that you can only provide a secure cloud solution if all internal processes and procedures are secured as well. That is why IXON has developed and implemented a comprehensive information security management system (ISMS).

IXON's ISMS is certified according to the ISO 27001 standard: the leading global standard for information security in organisations. It requires adherence to a number of disciplines, including access control, (cyber)security, compliance, risk management and business continuity. Compliance with ISO 27001 shows that organisations have implemented comprehensive security programs and controls that protect their information and those of their customers in accordance with internationally recognized standards.

The ISMS covers all of IXON's business activities:

- ☑ Development of cloud connectivity solutions for machines and devices
- ☑ Gateway production for connecting machines and devices to the IXON Cloud platform
- ☑ Management and maintenance of the IXON Cloud platform
- ☑ And selling and supporting IXON products and services

Choosing such a wide scope for the ISMS allows protection of not only all data in the IXON Cloud, but also all of the internal company data. Thanks to the ISMS, IXON can protect the confidentiality, availability and integrity of all data.

Extensive audits

After a series of extensive audits by DigiTrust in 2018, a certification body accredited by the Dutch accreditation board (RvA), IXON's ISMS was found to be fully compliant with the ISO 27001 standard. Annual audits by DigiTrust ensure that IXON's ISMS remains up-to-date with all latest (cyber)security standards.

DigiTrust
CERTIFICATION OF QUALITY SYSTEMS

CERTIFICATE

Certificate of Registration

This certificate with registration number DGT2019011401 has been issued for the Management System of:

IXON B.V.
Located at: Vierlingsbeekseweg 52A, 5825 AX at Overloon, The Netherlands

Standard:
ISO/IEC 27001: 2013

The Information Security Management System is applicable to the following: "Development of cloud connectivity solutions for machines and devices. Gateway production for connecting machines and devices to the IXON cloud platform. Management and maintenance of the IXON cloud platform. Selling and supporting IXON products and services.".

The selection of mitigation measures is described in the Statement of Applicability version 1.4, dated November 16th, 2018.

This certificate is valid from: January 14th , 2019
This certificate is valid until: January 14th, 2022
Date first certificate: January 14th, 2016
This certificate replaces number: ---

M.C. Bijl
DigiTrust B.V.

MGMT. SYS. RvA C 618

DigiTrust B.V. Jean Monnetpark 11 – 7336 BA Apeldoorn – The Netherlands
Phone: +31 (0)88 22 45 600 - info@digitrust.nl - www.digitrust.nl - KvK 59396822

Digitrust is geaccrediteerd door de Raad voor Accreditatie voor de norm ISO/IEC 27001

This certificate is issued in accordance with the Digitrust procedures and monitored by the RVA. This certificate was issued electronically and remains the property of Digitrust and is bound by the conditions of the contract. Certificates can be validated on the website of DigiTrust.

Figure 1. ISO 27001:2013 certificate belonging to IXON B.V.

Audits by DigiTrust

This shows the ISMS is of excellent quality and that IXON protects all data according to the highest industry standards. IXON will continue to improve the ISMS to ensure compliance with the latest industry best practices and technological advancements. This will be verified on a regular basis through internal audits and external audits by DigiTrust. With the ISO 27001 certification, IXON can now focus on driving innovation, with the confidence that all data is protected.

The IXON Cloud

This chapter will explain how the IXON Cloud is designed and what security measures are built in the IXON Cloud platform. Firstly, the services and servers that comprise the IXON Cloud are detailed. Secondly, the security controls of the IXON Cloud are discussed.

Services and servers

The IXON Cloud is a complex network of over 60 servers, distributed worldwide. It is structured to provide the best performance, availability and security. It consists of numerous server and database types, of which the key types are discussed below in more detail. Its servers are hosted at several industry-leading hosting providers (for segmentation and stability reasons), which uphold the highest security standards and have obtained ISO 27001 certifications.
All servers which store or process data are located in the European Union and are subject to GDPR-guidelines. The exact domains and locations of servers are in constant change to ensure the latest configurations, software and tools are used.

> "Note that IXON does not own any data stored by users in the IXON Cloud; all data is owned by its users."

API services

The application programming interface (API) services are the heart of the IXON Cloud and are located in data centers in Amsterdam. They handle key processes in the IXON Cloud, including authorizing and configuring VPN connections and connecting to our databases.

The API services are not publicly accessible, but can be used by IXON Cloud users after a unique API key is provided by IXON. Users are then able to use the API services for creating custom applications or integrations with third parties.

MQTT broker services

The IXON Cloud uses the Message Queueing Telemetry Transport (MQTT) protocol for data transfer. The MQTT protocol is ideal for the Industrial IoT, because it is highly efficient, secure, has minimal overhead and greatly diminishes bandwidth use.

IXON's MQTT broker services are used for pushing router configurations, firmware upgrades and for the transmission of Cloud Logging and Cloud Notify data. The MQTT broker services are physically located in data centers in Amsterdam.

VPN servers

IXON's VPN servers are located in data centers around the world to provide low-latency connections. The VPN server network is redundant, so if one VPN server goes down, the other servers will take over automatically. The API decides which VPN server is best for setting up a secure VPN tunnel, based on the physical location of the IXrouter and its nearest VPN server. All you need to do is install our VPN client (IXclient) for setting up a secure connection from your browser to your machine.

Our VPN client is a lightweight application, running in the background on your computer, that enables you to set up a secure VPN connection to your machine from within your browser.

Even for devices that do not have the VPN client, it is still possible to access the HMI or web-based controls of your machines. With Cloud Access, the machine data is sent through the IXrouter to the VPN server using the already established VPN connection, and that information is then streamed to your browser using HTTPS or a secure WebSocket connection.

Figure 2: IXON Cloud data center locations across the globe.

Kubernetes cluster

The IXON Cloud platform contains multiple Kubernetes clusters for enabling and managing microservices. This modern architectural style ensures optimal scalability and availability of the IXON Cloud platform. Microservices allow large applications to be structured as a collection of loosely coupled, smaller applications (services) that can be managed and updated individually, without downtime. Each microservice is built as a Docker container and Kubernetes is used for managing all these microservices.

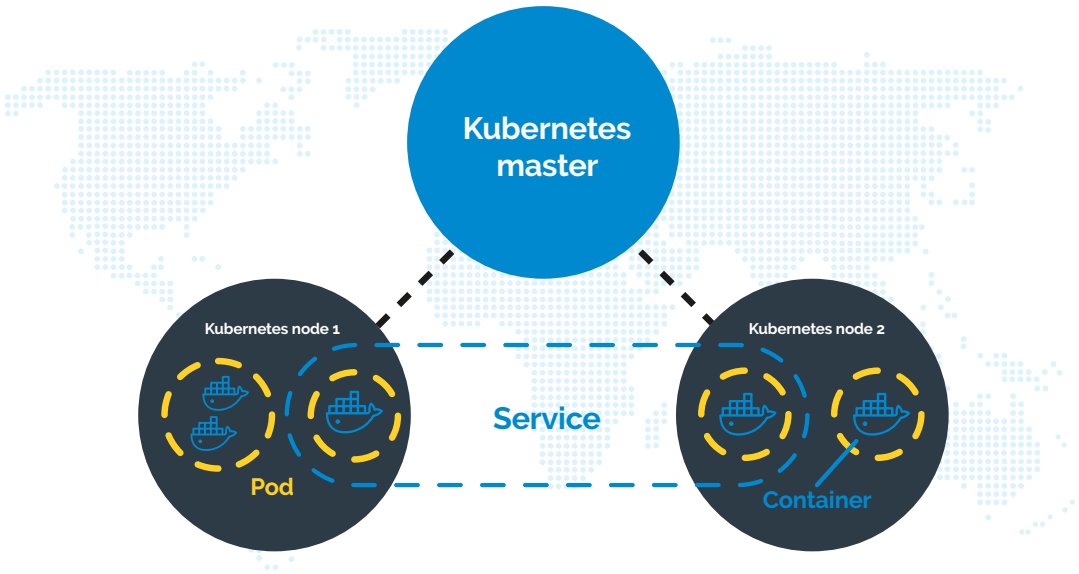


Figure 3: Kubernetes cluster. The Kubernetes master acts as a manager for Docker containers. It can manage and update these containers individually, in order to build a modern, fast and scalable application.

Relational database cluster

The relational database stores information about IXON Cloud users, companies, devices, etc. It is set up redundantly using a master-slave structure across multiple data centers in Amsterdam. The Master receives and processes all requests to view or edit the database.

The Slave replicates all write/update events on the Master and creates a backup every four hours. In case of any issues with the Master, the roles can be switched to ensure database availability. Only the IXON API, Slave and Kubernetes cluster are able to communicate with the Master; all other connections are refused outright.

Non-relational database cluster

The non-relational database stores data on IXON Cloud platform events, generated alarms, logs, etc. This database is configured as a replica set, of which the primary server receives and processes all requests, and the secondary server replicates the primary server. This configuration ensures high availability and redundancy. Only the IXON API, other servers in the replica set or Kubernetes cluster are able to communicate with the non-relational database; all other connections are refused outright. The database servers are located across multiple data centers in Amsterdam.

Time series database cluster

Machine data gathered with Cloud Logging is sent using the lightweight and highly efficient MQTT protocol. After the IXrouter collects the data, it is first passed to our MQTT broker: a central station for receiving and sending data messages. There it is timestamped and stored in a buffer database. Next, a time correction is applied to account for any possible discrepancies between the IXrouter's internal clock and the NTP time (actual time).

Finally, the data is stored in a time series database cluster, which is hosted in a data center in Frankfurt, Germany. The main advantage of a time series database is that it's optimised for handling timestamped data. This allows users to request data over a large period of time in just a few milliseconds and perform operations, such as calculating the mean value, in a fast and highly efficient manner. Furthermore, time series databases allow for advanced data lifecycle management options, such as aggregation or downsampling of your machine data.

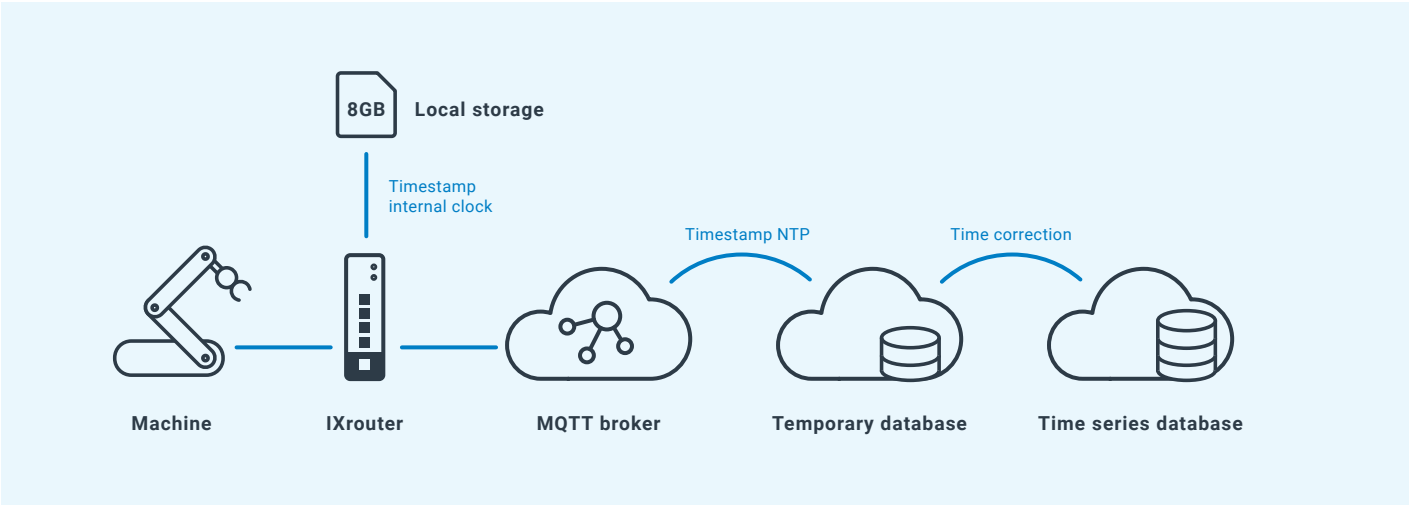


Figure 4. Machine data: the road from machine to the IXON Cloud.

Figure 5. Dylan Eikelenboom, security officer at IXON.

Security controls

Security officer

As an organisation that prioritizes security, it is imperative to have someone responsible for and fully dedicated to this topic.

IXON's security officer, Dylan Eikelenboom, is head of the Security team and is responsible for securing the IXON Cloud.

He works in close collaboration with operational management, IT management and process management. This guarantees that security is an integral part of IXON. His main tasks include monitoring the IXON Cloud, vulnerability management, redundancy, and ensuring overall security is in line with the highest industry standards.

Encrypted connections

Encrypted connections are necessary to prevent attacks which can let attackers gain access to accounts and sensitive information.

All connections to and from the IXON Cloud and between Cloud services are therefore encrypted using HTTPS with TLS 1.2 or higher. MQTT connections are also TLS encrypted to ensure the confidentiality of your machine data. VPN connections use single-use VPN certificates and are encrypted using AES-256-CBC with SHA512. IXON Cloud user passwords are stored as hashes using PBKDF2 with 12 bytes salt, 12000 iterations and SHA512 + HMAC. These strong algorithms help to establish a secure connection.

Server hardening

Every server of the IXON Cloud is deployed using a base configuration that has been hardened against cyberattacks in a number of ways. As a non-exhaustive list, all servers:

- ☑ automatically install and deploy security updates.
- ☑ employ a firewall that, by default, blocks all unnecessary traffic.
- ☑ install and update all cybersecurity tools (i.e. for monitoring, auditing and logging).
- ☑ limit SSH access to known usernames and SSH keys.
- ☑ And much more.

Centralized monitoring, logging and analysis

The IXON Cloud is monitored 24/7 and logs are stored and analyzed on a centralized logging platform. The centralized logging platform is mainly focused on collecting information about employee actions on IXON's systems, server performance and database requests. It uses artificial intelligence to detect critical events and anomalies in real time before they affect users. IXON's security officer is tasked with analyzing all monitoring and logging reports in order to quickly identify and react to any performance issues, unusual server activity or unauthorized actions.

Vulnerability management

A third-party vulnerability solution scans the IXON Cloud weekly for any external vulnerabilities. Scan results are reported in a centralized overview and assessed by the security officer. In addition, IXON's servers are audited daily by another third party specialized in server security and system hardening. Server auditing is aimed at determining system health by detecting any internal vulnerabilities or configuration management weaknesses.

A centralized overview of the audit results shows the status of each server and provides guidance for improvement. This enables IXON to quickly react to any new vulnerabilities and to confirm that each server matches the highest security standards.

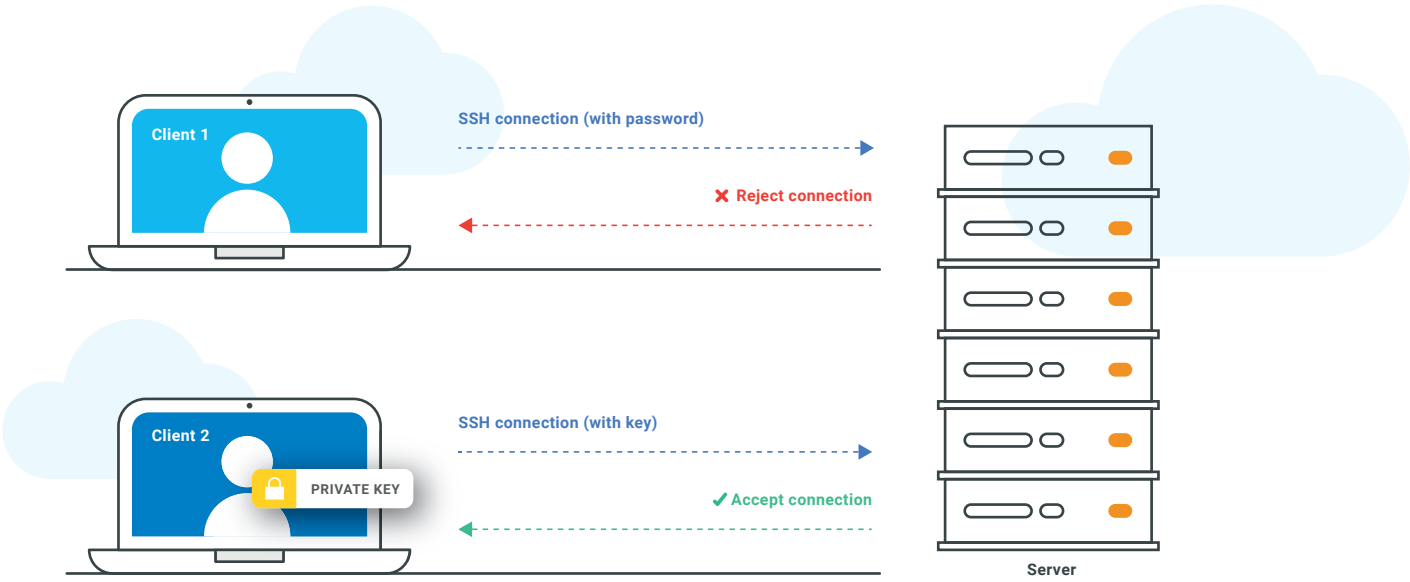
Furthermore, at least once a year, both the IXON Cloud and the IXrouter are subject to a thorough penetration test by a company specialized in ethical hacking.

Detected vulnerabilities are scored for three criteria, 1) the ease to exploit the vulnerability, 2) the current impact of the vulnerability, 3) the likelihood that the impact will increase in the near future.
The resulting risk score determines the priority to fix the vulnerability
according to the following scheme:

Risk	Response time
Negligible	Not specified.
Low	Not specified.
Medium	Development starts within 2 months. Fixed within 3 months.
Severe	Development starts within 2 working days. Fixed within 2 weeks.
Critical	Development starts immediately. Fixed within 48 hours.

Access control

IXON has implemented a strict control policy for accessing servers. Only a few of IXON's senior developers are able to access the IXON Cloud's servers. Other developers may be given access to a server temporarily, if this is necessary for their task, under the direct supervision of a senior developer. Developers log into servers using their own unique digital version of a house key, their SSH key. All server logins and changes are monitored 24/7 and logged to the centralized logging platform for analysis.



> "We implemented a strict control policy for accessing servers."

Software development security

IXON's software development life cycle is focused on delivering secure, high quality software. All software is tracked through an advanced software versioning management system. New code is developed following language-specific coding conventions and secure coding techniques.

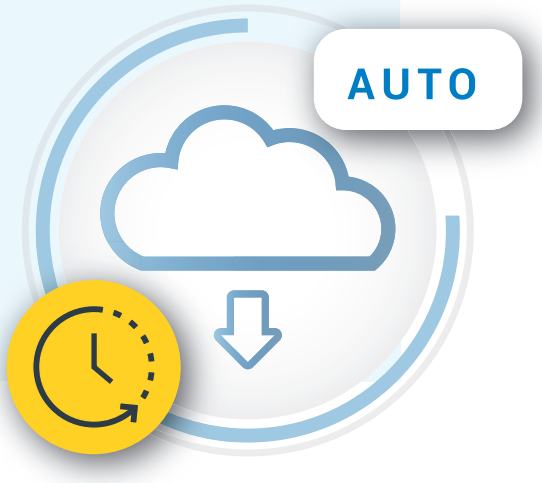
All software changes are reviewed by at least one other developer and are thoroughly tested through manual and fully automated tests. IXON's software versioning management system has been designed for continuous integration, delivery and deployment. This means that for most software updates, all code is:

- Automatically tested with 100% code coverage;
- After all tests have passed, software changes are automatically scheduled for release, and;
- Software is then automatically released, without human intervention.

This method of automated testing and releasing software changes greatly reduces risks for each release and enables developers to get valuable features and improvements out fast and in a sustainable way

Backups

All data that exists in the IXON Cloud is backed up using automated systems. For customer data, a backup is created every 4 hours and retained indefinitely. For Cloud logging data, a backup is created every hour and backups are retained for 7 days. IXON's senior developers can access these in a disaster recovery event.



IXrouter security

To connect your machine(s) to the IXON Cloud you have to use the IXrouter. This chapter discusses all safety measures that IXON has taken to ensure that the IXrouter establishes safe connections.

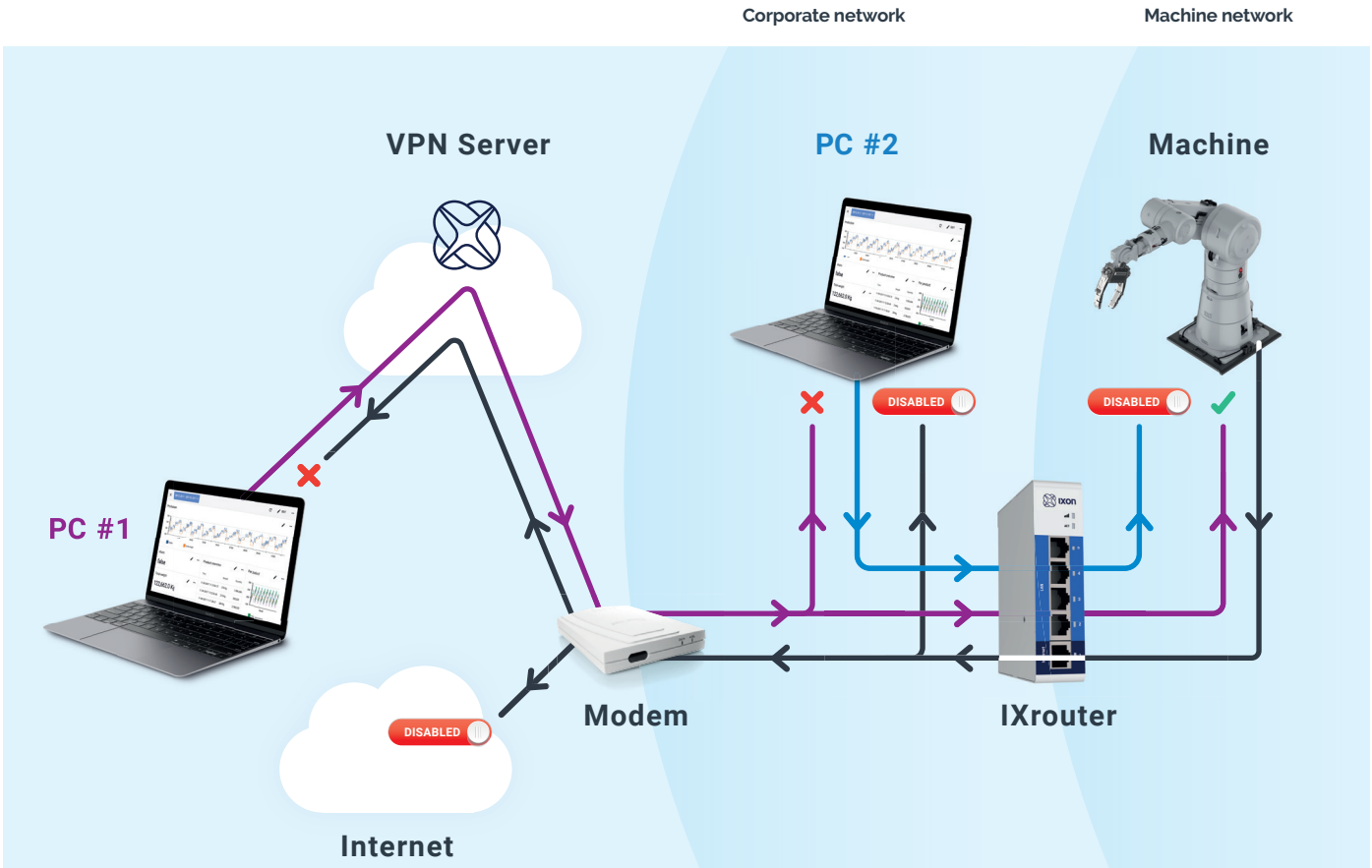
Built-in firewall separates your machine from the internet

Machine controllers were never designed for security. Their operating systems are not updated and do not contain the latest security mechanisms. It is imperative that these machine controllers are never connected to a company network while linked to other devices. The IXrouter can isolate these from the company network with its built-in firewall.

The IXrouter is a robust and compact industrial router, the edge gateway that connects machines to the IXON Cloud. Its built-in firewall completely separates the WAN port (company network) from the LAN ports (machine network). It blocks all communication except for authorized and encrypted data verified by a valid identity certificate. This means that only authorized users can access the machine network via the IXON Cloud.

> "The firewall blocks all traffic from the WAN to the LAN ports - and vice versa - by default."

What is and isn't accessible



From		To	Mode	Accessible?
PC #1	›	Machine	VPN	✓
PC #1	›	PC #2	VPN	✗
PC #2	›	Machine	TCP	DISABLED (1)
Machine	›	PC #2	TCP	DISABLED (1)
Machine	›	Internet	TCP	DISABLED (1)
Machine	›	PC #1	VPN	✗

(1) Disabled by default. Configurable in the IXON Cloud platform.

Outgoing ports

The IXrouter only uses outgoing ports to establish a secure connection to the IXON Cloud, so there is no need to open any incoming ports on the local firewall in the company network..

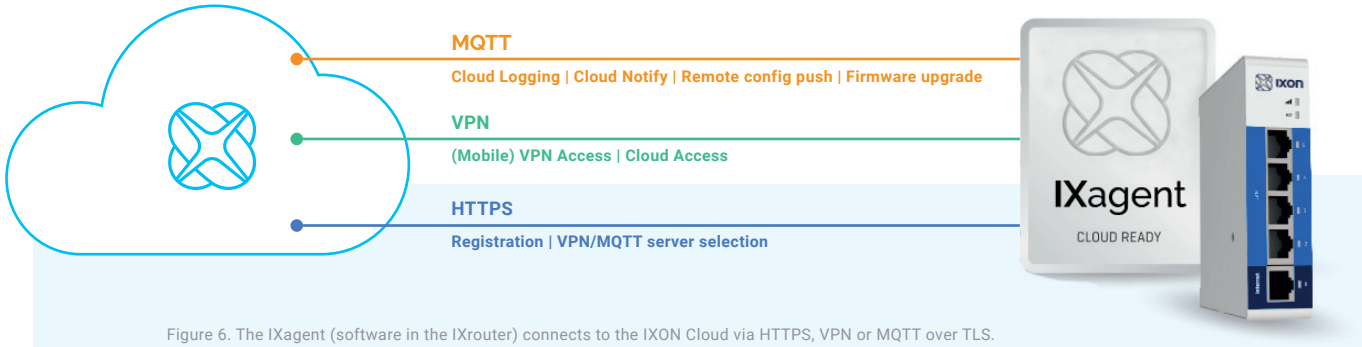


Figure 6. The IXagent (software in the IXrouter) connects to the IXON Cloud via HTTPS, VPN or MQTT over TLS.

The IXrouter is only able to connect to IXON servers with a domain ending in .ixon.net, .ixon.cloud and ayayot.com. Below is an overview of the outgoing ports and protocols that the IXrouter utilizes.

Port	Transport	Application
443, 8443 (1)	TCP	HTTPS, MQTT (TLS), OpenVPN
53 (2)	TCP & UDP	DNS

(1) Port 8443 is only used when stealth mode is activated for connectivity via a censored internet connection (i.e. when located in China).

(2) DNS requests are often handled by local DNS servers. In those cases the listed DNS port can be ignored.

Access restriction that meets customers' security standards

The local IT department may choose to only grant specific devices internet access, based on the MAC address or IP address of the device. The MAC address can be obtained from the label on the side of the IXrouter or from the info panel in the IXON Cloud. The IP address can be set to a static IP address. However, by default the IP address is set to be obtained automatically via DHCP.

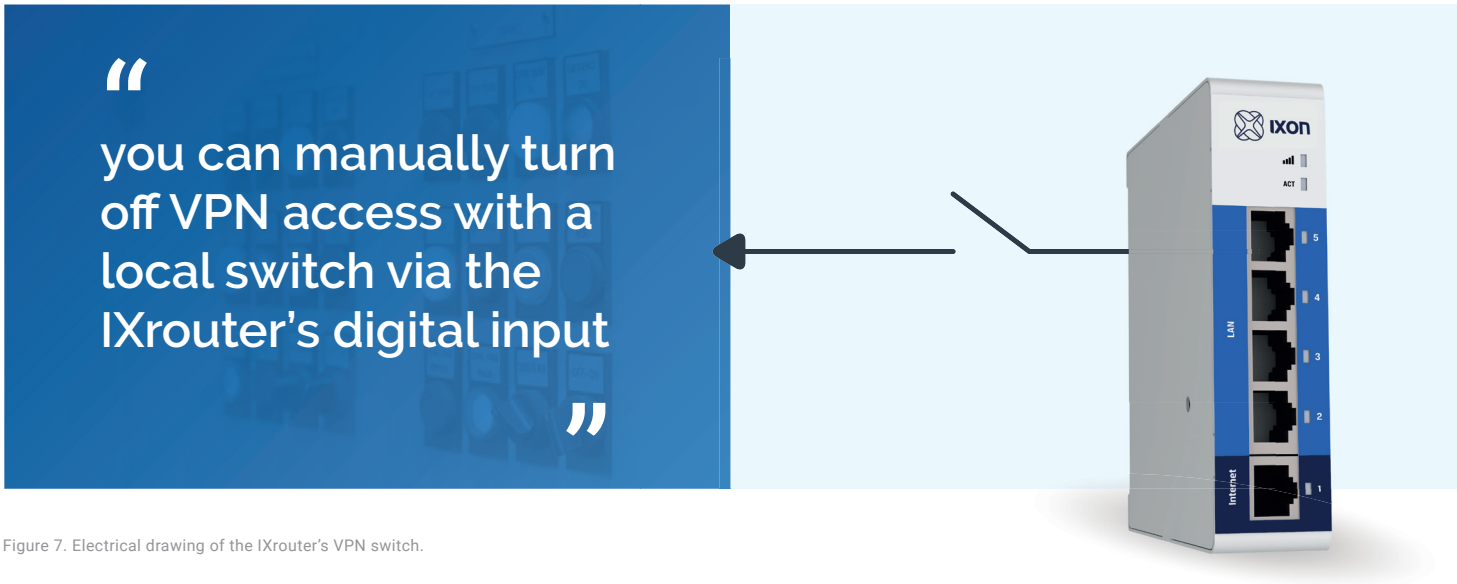


Figure 7. Electrical drawing of the IXrouter's VPN switch.

Always keep your machine online with the IXrouter failover

Should your preferred connection drop, the IXrouter will automatically connect to another network. This is fully configurable for Wi-Fi, 4G, and Ethernet. Each connection is checked by sending keep-alive messages to a public IP address every few seconds.

If the connection fails multiple consecutive times, the connection is considered down and the IXrouter will automatically connect to the first (or second) fallback. If the preferred network is up again, the IXrouter will automatically switch back to the preferred network. The IP address for keep-alive messages and time interval can be changed according to individual needs

Data logging even when your machine is offline

Internet connections are not always stable and may go down from time to time. In some situations, such as on a ship, there might not even be an internet connection available at all. This is problematic for users who wish to log their machine data in such conditions.

To solve this, the IXrouter has an 8GB flash memory which allows machine data to be stored offline for weeks at a time. As soon as the IXrouter comes back online again, all machine data is automatically sent to the IXON Cloud over an encrypted connection.

Additionally, users are able to receive notifications when the IXrouter has been offline for a specified number of hours with the Cloud Notify functionality. This allows users to quickly react to any connectivity problems and fix these issues as soon as possible.

Hardware certifications

The IXrouter's certifications ensure IXON hardware products match the highest safety, health and environmental protection standards. The IXrouter has been certified for:

- CE certification
- FCC verification
- cULus listing (E492721)

> "Furthermore, the IXrouter is fully compliant with REACH and RoHS regulations and is completely asbestos-free."

Browser and app security

In this last chapter the security precautions for our browser and mobile applications are discussed.

Login security

The IXON Cloud platform can be accessed via any web browser or via the IXON app on your mobile device. Users log in with their username and password. If two-factor authentication is enabled, users are also prompted to enter a one-time password. One-time passwords add an extra layer of security to your account. They are generated by an app (e.g. Google Authenticator) on your mobile device and remain valid for 30 seconds.

Unsuccessful login attempts return the user to the login screen. After five incorrect attempts, the user is locked out of his/her account for a number of seconds. This time increases exponentially (up to 1 hour) with subsequent incorrect attempts.

User management

From the IXON Cloud admin application, access to certain apps, machines or services of the IXON Cloud platform can be managed based on the role of users within one company. Additionally access can be managed for different groups to further regulate access based on for example the company of an end customer, a machine type or geographic region.

> “The IXON Cloud platform can be accessed via any modern web browser or via the IXON app on your phone.”

A safe, reliable and trustworthy IIoT solution

With the IXON Cloud, IXON offers machine builders a highly secure and advanced Industrial Internet of Things platform. Comprehensive security controls and redundant servers worldwide are key in achieving a safe, reliable and trustworthy IIoT solution. Protecting your information is our top priority and we will do anything to secure your data, following industry best practices.

Over 1000 companies across the globe trust IXON with their most valuable asset: information. IXON will continue to invest in security and new innovations to allow IXON Cloud users to benefit from its full potential in a secure manner.

For more information about security, please contact our security officer, Dylan Eikelenboom:

Email security@ixon.cloud
Phone +31 (0)85 744 1105

www.ixon.cloud →