# Secure Remote Access for OT

## Enabling Zero-Trust Network Access (ZTNA) in Operational Spaces

## Overview

Remote access is key for operations teams to manage and troubleshoot Operational Technology (OT) assets at scale without time-consuming and costly site visits. Industrial equipment—from roadside cameras to robots on the manufacturing floor—frequently requires specialized technical support from their respective manufacturers or remote experts. However, the increasing need for remote connectivity to critical equipment opens the attack surface to threat actors, and if implemented incorrectly, can lead to a breach.

Remote access solutions come in many forms, and it can often be confusing to understand which one will meet business needs. This solution brief is a high-level overview of the reference architecture described in the Cisco® Validated Design dedicated to secure remote access for industrial networks. It is a fully tested and validated solution addressing critical business challenges. The design provides comprehensive guidance, with configuration steps that help ensure effective, secure deployments for our customers.



Cisco Validated Design

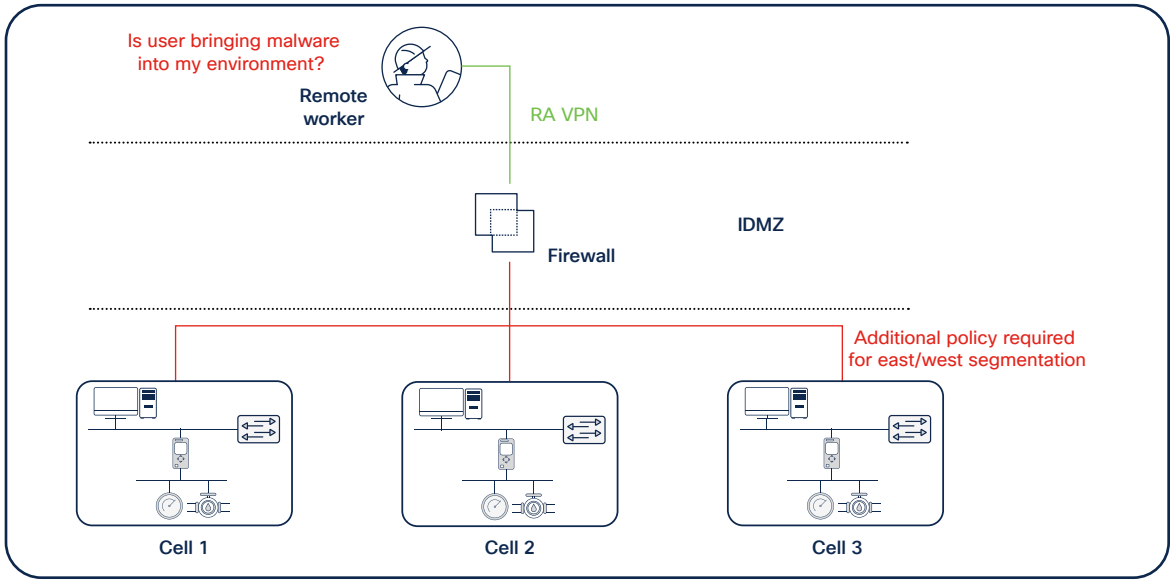
## Benefits

- Provides remote access to specific devices, never to the full network.
- Simplifies deployment by avoiding complex DMZ/ firewall setups.
- Enables access to be scheduled during maintenance windows.
- Protects against the threat of stolen credentials with multifactor authentication.
- Blocks access from risky devices that fail a device posture check.
- Monitors and terminates active sessions.
- Records sessions to enable investigations.

# Challenges with existing remote access solutions

Using VPNs is a widespread practice when connecting remote users, but if not configured correctly, they can give unrestricted access to the network. With what is known about the risk of stolen credentials, a multifactor authentication solution should be used for any remote access solution. However, a VPN extends the network to the remote user, which brings their machine in as a remote client. If the machine is not scanned before access is given, malicious software could unintentionally be introduced to the OT network.

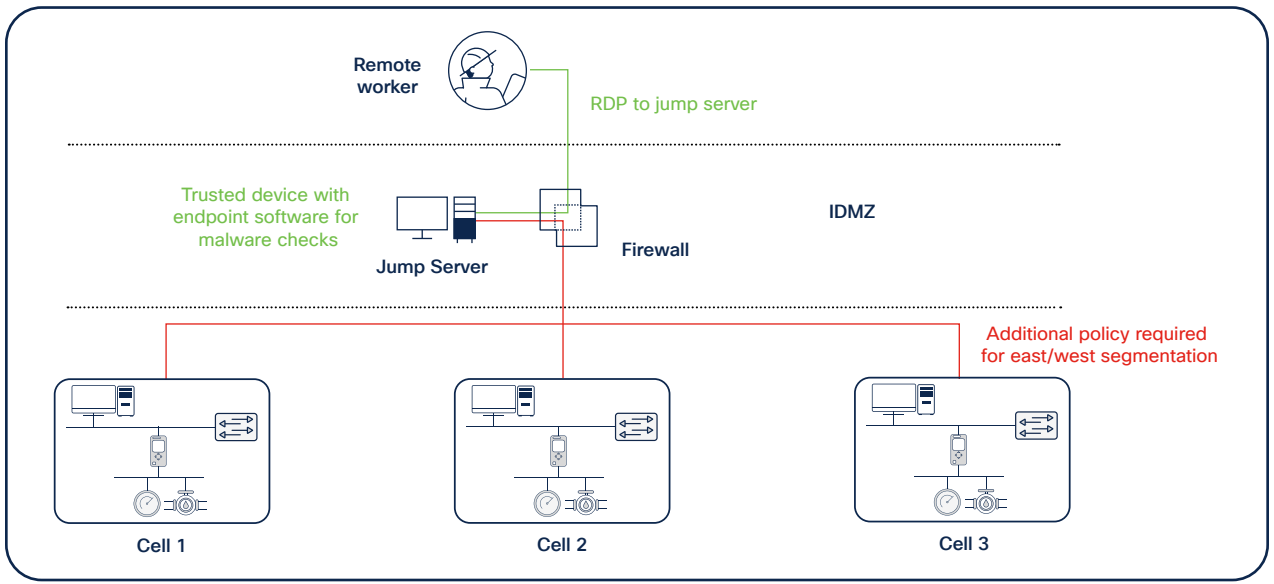
Figure 1. Security policies are needed to restrict what users can do over the VPN



Further, with a VPN solution, additional access control needs to be placed on the user to limit their actions to a predetermined scope of work. In the case of a vendor who is performing maintenance in a production environment, the vendor needs access to a single machine during the duration of a maintenance window and should not have the ability to laterally move to any other machine, whether intentionally or unintentionally.

One method of reducing the scope of a remote user is to force them to interact with the network using a jump server. Policies placed on the firewall will help ensure that all activities performed on the OT network originate from the jump server, which is a trusted device fully controlled by the networking team. While jump servers solve the challenge of malicious software being introduced to the network by a remote device, they do not help control what a user can do once they have access to the jump server.

Figure 2. Jump servers help control malicious traffic, but security policies are still needed




Best practices would leave jump servers in a quarantined state, where they are denied any access to the OT network until called upon. As necessary, security administrators will open specific policies to control what a user can and cannot do from that server. The operational burden can be overwhelming, often impossible, and in reality, jump servers expose themselves to the same frailties as the VPN solution.

# The shift to zero-trust network access for OT

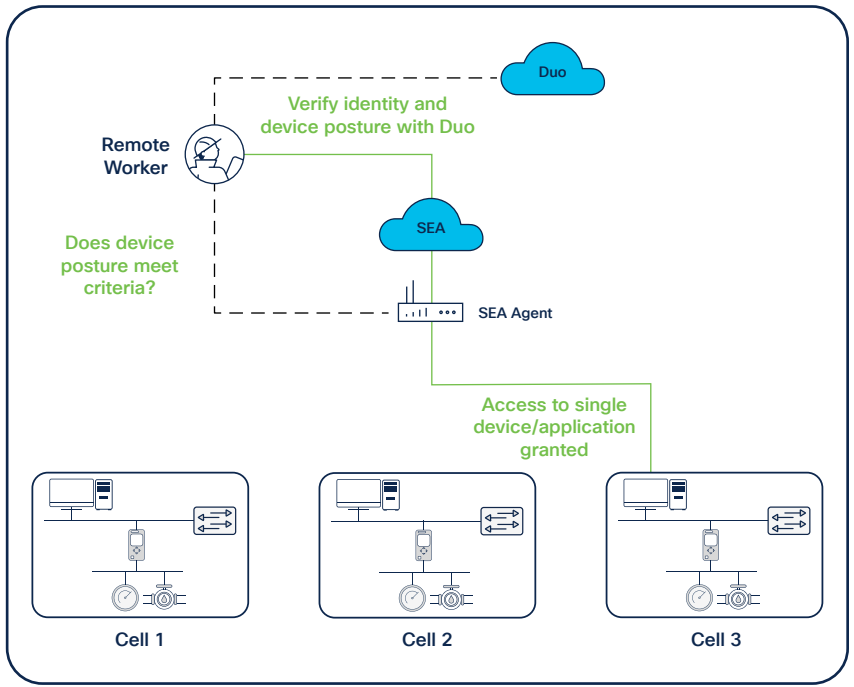
Zero-Trust Network Access (ZTNA) is a security service that verifies users and grants access to specific applications based on identity and context policies. Zero trust can be summed up as “never trust; always verify.” ZTNA solutions connect authorized users directly to applications rather than to the network—and only to those applications they are authorized to access on need-to-know-based policies.

Cisco has developed a ZTNA solution specifically designed to meet OT constraints and industrial workflows. Cisco Secure Equipment Access is a cloud service that works with a software agent installed on Cisco networking equipment to provide granular access controls to any assets using SSH, RDP, VNC, Telnet, HTTP/S, or VPN for desktop applications. Remote users connect to a cloud portal and have access only to the devices you choose, using only the protocols you specify, and only after they have passed a series of security controls. It can easily be managed by an operations administrator.

Adoption of zero trust can help address common security challenges in the workforce, such as phishing, malware, credential theft, remote access, and device security. This is done by securing the three primary factors that make up the workforce: users, their devices, and the applications they access.

For more information on Cisco Secure Equipment Access, please visit cisco.com/go/sea.

Figure 3. Cisco Secure Equipment Access is a cloud-delivered service that runs on your Cisco industrial network



# How it works

## Verifying users with Cisco Duo

Ensuring the trust of your users whenever they attempt to access applications remotely is the first step toward secure remote access. When using Cisco Secure Equipment Access, Duo helps mitigating the threat of stolen credentials:

- **Multifactor Authentication (MFA):** Authentication based on usernames and passwords alone is unreliable. Many reuse passwords across services and create passwords that lack complexity. Passwords also offer weak security because of the ease of acquiring them through hacking, phishing, and malware. MFA requires extra means of verification that unauthorized users will not have. Even if a threat actor can impersonate a user with one piece of evidence, they will not be able to provide two or more.
- **Single Sign-On (SSO):** SSO is an authentication process that provides users with one easy and consistent login experience across all applications, eliminating the need to supply user credentials with every application or access request. With SSO, security administrators can enforce strict user policies in a centralized location. MFA and user policy can be applied during SSO, eliminating the need to duplicate and maintain authentication policies across multiple applications, such as remote access software.

## Verifying device posture

If users are logging into your company's applications with outdated devices, there is a chance they could also be unwittingly spreading malware or using keyloggers to record your keystrokes. As a result, your industrial environment could be at risk if just one out-of-date device logs in.

To protect the network, Duo offers the following capabilities:

- **Device posture assessment:** Enforcing consistent security policies across managed, personal (BYOD), corporate-owned, personally enabled, and third-party (contractor or partner) devices poses a significant challenge. Duo's device posture assessment analyzes the device and assesses its security posture before allowing remote access to your applications. It gives IT security teams the insight and an enforcement mechanism to automate access decisions on endpoints, particularly among unmanaged devices.
- **Anti-malware:** Advanced malware's goal is to penetrate a system and avoid detection. Once loaded onto a computer system, it can self-replicate and insert itself into other programs or files. Enforcing anti-malware protection in the endpoint helps to prevent endpoint infection and remove unwanted threats attempting to enter the environment during a remote access session. When using Duo's Cisco Secure Endpoint integration, remote access is denied for devices identified as "compromised." You can gain peace of mind that use cases such as file transfer from remote users to OT devices will not contain hidden malware and cause a breach by an unwitting threat actor.

For more information on Cisco Duo, please visit duo.com.

# How it works

## Least-privilege access control

Zero trust requires that a user be given access only to the applications they truly need to do their job—and no more. This granularity helps ensure that access is provided only to users or groups of users who need it, from locations and devices that are trusted. To protect the network from discovery, lateral movement, and impaired process control, Cisco Secure Equipment Access provides the following capabilities:

- **Identity authorization:** Establish trust by verifying user and device identity at every access attempt. Least-privilege access is assigned to every user and device on the network, meaning only the machines, network resources, and workload communications that are required are permitted. Access to the full network is never granted.
- **Time-based access:** Remote access should not be an always-on feature. Access should be granted only when needed and restricted to the resources required for a given access attempt. Cisco Secure Equipment Access provides the ability to grant access only at time of need, for a specified period, before being turned off by the system. If a session expires beyond the allocated window, a new session must be created.

## Auditing

Many compliance standards require that an audit trail be maintained for all activity that occurs from remote networks. Between Cisco Secure Equipment Access and Duo, the following capabilities are provided:

- **Authentication logs:** Authentication logs show you where and how users authenticate, with usernames, location, time, device posture, and access logs.
- **Administration logs:** Administration logs show you the sessions that were created, who created them, and what access control measures were put in place for the end users.
- **Session monitoring:** An administrator can join a remote session and view in real time what is happening. For example, when a technician delivers remote support for an asset, an OT operator may want to oversee the actions taken.
- **Session termination:** An administrator can terminate an active session either that should never have become active in the first place or in which the remote user being monitored attempts to deviate from their permitted actions.
- **Session recording:** Remote sessions can be recorded and stored for use in an audit trail. If a breach were to occur, having the ability to go back and watch what remote users did to a system aids incident investigation.

## Learn more

For more details on Cisco's remote access solution, read the Secure Remote Access for Industrial Networks Design Guide. You can also talk to a Cisco sales representative or channel partner and visit cisco.com/go/iotsecurity or cisco.com/go/sea.

## The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe to digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It is a rare combination.



C22-3859501-00 09/23