WHITE PAPER

Secure Access for Operational Technology at Scale

Enabling Remote Work and Ensuring Business Continuity

Executive Summary

Operational technology (OT) makes it possible for factories, power generation and transmission facilities, public transportation networks, oil and gas facilities, and utilities to function. Because these organizations provide critical products and services, they need to have a business continuity plan.

Fortinet offers an integrated solution for secure remote access that addresses the needs of OT. FortiGate Next-Generation Firewalls (NGFWs) have built-in support for IPsec virtual private networks (VPNs), which enable remote workers to connect securely to the company network from alternate work sites, whether they be company IT or OT networks. With endpoint protection provided by FortiClient and FortiToken, multi-factor authentication (MFA), combined with FortiAuthenticator single sign-on (SSO), organizations can securely support remote work and maintain business continuity. FortiPAM can be used to provide credential vaulting, zero-trust access and monitoring, and reporting of access to organizations' most critical OT devices for privileged users.

Three out of four OT organizations experienced at least one system intrusion in the past year.[1]

Maintaining Operations through Remote Work

Many OT organizations are critical to public safety, so these organizations must ensure that they can maintain operations in the face of adversity and potential emergencies, such as illness, flood, hurricanes, and power outages.

In developing a business continuity plan, an important consideration is that the organization may not be capable of sustaining normal operations on-site. The ability to securely support employees working remotely is essential to ensuring OT business continuity. OT organizations also need secure remote access because they may need to commission new equipment, apply critical patches, or deal with repairs and troubleshooting activities remotely. Additionally, OT organizations may perform remote monitoring and diagnostics or use remote operation centers to affordably take care of geographically distributed assets. Security is critical because a breach in an OT environment could lead to outages of services and the loss of human life or damage critical infrastructures.

Fortinet solutions are easily deployed to remote work locations. However, many organizations also require resources on-site or in the cloud to securely support remote workers. In many cases, organizations already have these resources in place because they are part of their existing security infrastructure. In the event of a natural disaster or other event that disrupts normal business operations, an organization must be capable of rapidly transitioning to a fully remote workforce. Beyond offering encryption of data in transit using a virtual private network (VPN), Fortinet solutions offer several other features that can help an organization secure its hybrid workforce and infrastructure.

These features include:

- **MFA and SSO:** FortiToken and FortiAuthenticator enable dual-factor authentication and single sign-on for remote employees and third parties.
- **NGFW and intrusion prevention system, antivirus, web filtering, and software-defined wide area networking (SD-WAN):** FortiGate provides all of these features and more in a single appliance.
- **Wireless connectivity:** FortiAP and FortiExtender provide secure wireless access, including cellular wireless 3G, 4G LTE, and 5G connections at remote work locations with full integration and configuration management in a single pane of glass.
- **Privileged user access:** FortiPAM provides credential vaulting and password change capabilities along with zero trust, posture checking, and monitoring of access by privileged users to critical OT systems.

A FortiGate NGFW is capable of inspecting encrypted and plain-text traffic at an enterprise scale with minimal impact on performance. FortiGate NGFWs also include an integrated VPN gateway that acts as an endpoint for encrypted connections to remote workers. FortiGate NGFWs running FortiOS 7.0 also have zero-trust network access (ZTNA) built in. ZTNA is a way of controlling access to applications regardless of where the user or the application resides. ZTNA is the natural evolution of VPN and offers better security, more granular control, and a better user experience, so it can be a good option for securely connecting a remote workforce.

The FortiGate NGFW also integrates with common IT infrastructure elements, including corporate directory services, such as Microsoft Active Directory (AD) and MFA and SSO solutions. FortiAuthenticator provides a single, centralized integration point for authentication solutions and supports third-party solutions as well as FortiToken, which offers hardware, software, and email-based token options. The software tokens are supported for a variety of smartphones and mobile devices.

Because the FortiGate VM virtual appliance can perform at 20 Gbps on AWS and other cloud services using large instance types, it can support thousands of remote users, regardless of whether they use FortiClient or other third-party VPN clients. Many sites use FortiGate VM to securely connect to a public cloud-based security services hub to access applications that are in the cloud. Access to on-premises applications is also available through the closest cloud region and on to the private data center, which provides continuous support for high-speed data transfers from the cloud to data centers and vice versa.

FortiGate NGFWs and FortiAP wireless access points include zero-touch provisioning; they can be preconfigured before they ship so they can be automatically set up on-site.

Securing the Remote Workforce with FortiGate NGFWs

The high-performance IPsec and secure sockets layer (SSL) VPNs and ZTNA integrated into every FortiGate NGFW offer a flexible deployment model for both IT and OT organizations. Work-from-anywhere (WFA) users can either take advantage of a clientless ZTNA or VPN experience or gain access to additional features through a client-based VPN or ZTNA with the FortiClient endpoint security solution. Company employees and third-party vendors can also benefit from deploying a FortiAP wireless access point or FortiExtender wireless WAN extender combined with a FortiGate NGFW for wireless capabilities.

Fortinet solutions are designed to be easy to use from initial purchase through end of life. Both FortiGate NGFWs and FortiAP include zero-touch provisioning. Appliances deployed at remote sites can be preconfigured before they ship so they can be automatically set up on-site. Zero-touch provisioning helps ensure business continuity and support for remote work because no one on-site has to do additional configuration beyond plugging it in and connecting the network wires. FortiGate NGFWs are available as both physical and virtual appliances, and the FortiGate virtual appliances can be hosted in both public and private clouds.

The OT-Aware Security Fabric takes advantage of the Fortinet FortiOS network operating system and an open application programming interface (API) environment to create a broad, integrated, and automated security architecture. With the Fortinet OT-Aware Security Fabric, all of an organization's devices, including those deployed remotely to support hybrid work, can be monitored and managed from a central management platform. Security teams can achieve full visibility and control of all connected devices regardless of their deployment situation, either locally from a FortiGate NGFW or centrally from a FortiManager integrated centralized management platform deployed at the organization's headquarters.

Use Cases for Fortinet Products That Support Secure Access

Not every WFA employee in an organization requires the same level of access to company resources. And not every third-party contractor or vendor should be allowed access to a company's critical systems and networks without a formal authorization of remote access request and policing of remote connections. Fortinet provides tailored solutions for different types of WFA users.

1 Secure access for remote third parties, such as remote maintenance or monitoring and diagnostics (FortiClient, FortiToken, FortiAP, FortiGate, FortiPAM)

Remote third-party users may include maintenance engineers outside of the organization who maintain the industrial equipment. Sometimes they require a higher level of access to troubleshoot, operate, or manage industrial control systems (ICS) while working from a remote location. In the OT environment, they may need access to programmable logic controllers (PLCs) and remote terminal units (RTUs). They also may require the ability to operate in multiple, parallel IT environments. In some cases, remote third-party users include system integrators, industrial asset original equipment manufacturers (OEMs), vendors, and operators.

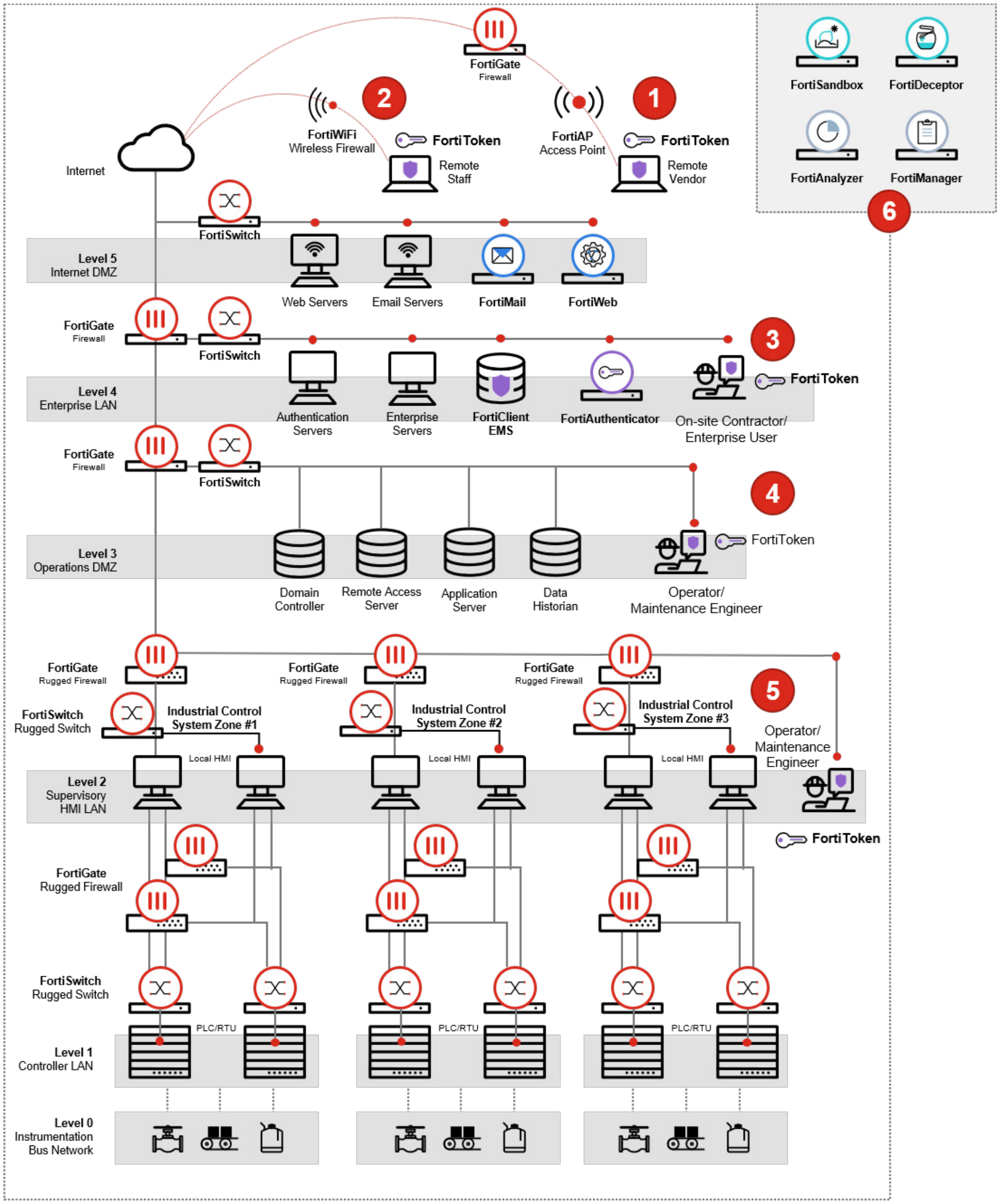

Figure 1: Secure access using Fortinet solutions across a connected IT and OT infrastructure

2 Secure access for remote staff, such as WFA employees (FortiClient, FortiToken, FortiWiFi, FortiPAM)

Remote employees need access to their company's systems to perform their day-to-day tasks. The remote access may include access to corporate enterprise IT capabilities such as email, internet, videoconferencing, file sharing, and function-specific capabilities such as access to finance or HR. For companies operating OT infrastructure, some of the employees may require access to OT systems for records and data retrieval and in some cases to perform maintenance and diagnostics. Employees who are responsible for the upkeep of the OT infrastructure must be able to remotely monitor the uptime performance of OT assets as well as perform basic troubleshooting on those assets in the event of an issue.

WFA employees can connect to both OT systems and corporate IT services using the FortiClient integrated VPN client software or ZTNA and verify their identity using a FortiToken for MFA.

3 Secure access for on-site contractors or enterprise users who need access to OT from IT networks (FortiClient, FortiToken, FortiGate, FortiClient EMS, FortiAuthenticator, FortiPAM)

Similar to use cases 1 and 2, on-site contractors and enterprise users may require access to OT systems from the IT enterprise network for data acquisition and maintenance purposes. However, the OT systems may be located in OT networks that are geographically dispersed across many sites. In some cases, the OT networks may be in remote locations where a personnel visit may not be possible because of travel restrictions or inhospitable site conditions.

The IT enterprise network may be located in a central location and can connect to the OT networks in different sites. In these situations, enabling secure access to the various OT networks from the central IT enterprise network can allow on-site contractors or enterprise users secure remote access to the OT systems. The central location can also provide a venue to implement centralized technologies for managing secure remote access such as centralized authorization and monitoring of remote access connections.

While complying with the regulatory mandates, secure access from the IT enterprise network to the OT networks may be required for audit and compliance purposes. Enterprise personnel may need access to OT networks to extract necessary information from the OT infrastructure to share it with regulatory bodies such as CERT organizations, NERC and FERC (as part of NERC CIP), and ENISA and CSIRT (as part of NIS-D). Below, use case six has more information on centralized reporting and management.

4 Secure access for operators or maintenance engineers who need ICS access from OT networks (FortiClient, FortiToken, FortiGate, FortiPAM)

Operators or maintenance engineers working in the control centers or control room may need to access the ICS assets for performing their routine operations, such as monitoring, diagnostics, and maintenance of ICS assets. The control center may be located in the same vicinity or far away from the ICS site. The network connection between the control center and the ICS site may be wired or wireless local area networking (LAN) or WAN.

Securing access and communication between the control center and ICS sites becomes paramount to prevent network attacks, such as man-in-the-middle and eavesdropping. To enhance the security measures for these access and networks, as part of the secure remote access implementation, features such as MFA for the access and encryption of network links can be implemented. Features such as SD-WAN can play an important role if the control center and ICS sites are connected using multiple communication links, and it's important to maintain the availability of these links cost-effectively.

5 Secure access for operators or maintenance engineers who need local ICS access (FortiClient, FortiToken, FortiGate, FortiPAM)

Secure access to the ICS assets doesn't always need to be from a remote site. In some cases, secure access may be required for the operators or engineers locally within the ICS sites to provision secure access to the ICS assets. This type of access can offer MFA and greatly improve the authentication, authorization, and accounting (AAA) capabilities for access to the ICS assets. Additionally, network encryption within the ICS networks can be implemented where necessary.

For large-scale secure access implementations, centralized management capabilities can greatly reduce the burden of managing multiple technologies and ease maintenance overhead should a need arise, such as updating software or firmware for multiple technologies.

6 Centralized security analytics, reporting and management, and centralized advanced threat protection (FortiAnalyzer, FortiManager, FortiSandbox, FortiDeceptor)

Whether secure access implementation is for local sites or remote sites, centralized logging, monitoring, reporting, and management for the implementation is important to obtain valuable information and efficiently manage the secure access infrastructure. Centralized implementation for logging, monitoring, and reporting can be done in the form of a network operations center (NOC) or security operations center (SOC).

In some cases, centralized reporting may be required for internal compliance purposes, such as reporting the information to the internal information security teams or board. Sometimes this information is critical to comply with the regulatory mandates, so the asset operator or owner may need to supply the information to the national or regional CERT communities.

For large-scale secure access implementations, centralized management capabilities can greatly reduce the burden of managing multiple technologies and ease maintenance overhead should a need arise, such as updating software or firmware for multiple technologies.

Additionally, to keep pace with emerging threats, advanced threat protection technologies, such as sandboxing tools, FortiSandbox and honeypots, and FortiDeceptor, can be implemented centrally to identify insider or outsider threats and mitigate risks.

Achieve Full Security Integration with Fortinet Solutions

When managing a remote and distributed workforce, centralized visibility and management of security infrastructure is essential. All Fortinet solutions can be integrated using the Fortinet Security Fabric, which provides a unified platform for visibility, configuration, and monitoring. Fabric connectors, an open API environment, DevOps community support, and a large extended security fabric ecosystem provide integration with more than 500 third-party solutions as well.

When an organization is preparing a business continuity plan, visibility and management across its security architecture are essential because the company may be forced to transition over to a fully remote workforce with little or no notice. Supporting remote work shouldn't jeopardize an organization's cybersecurity.

The following solutions are part of the Fortinet Security Fabric and support secure remote work and operations:

FortiClient has endpoint telemetry, vulnerability management, malware prevention, web filtering, application firewall, VPN client, ZTNA, and MFA support.

FortiClient EMS provides VPN client configuration, endpoint security policy, and profile management, and is a Security Fabric connector for centralized client deployment and management.

FortiAP delivers a secure connection with a wireless controller and extends networks to remote users. It eliminates the need for software VPN clients and offers zero-touch provisioning.

FortiExtender provides hybrid WAN-LAN connectivity, flexible wireless WAN connectivity, and supports cellular 3G, 4G LTE, and 5G networks. It is suitable for mobile sites, vehicle fleets, and field forces.

FortiWiFi and **FortiGate** are secure wireless controllers with VPN and ZTNA services that feature enforcement and admission control, NGFW, next-generation intrusion prevention (NGIPS), Security Fabric connectors, dynamic security policies, SD-WAN, and zero-touch provisioning.

FortiToken confirms the identity of users with hardware and software authentication tokens. It offers seamless integration with FortiGate and FortiAuthenticator with software tokens available for iOS and Android and safe and secure online activation with FortiGuard AI-Powered Security Services.

FortiAuthenticator provides authentication management with LDAP, RADIUS, and SAML integration, MFA and token management, hardware and software token support, and certificate authority.

FortiPAM provides privileged access management, control, and monitoring of elevated and privileged accounts, processes, and critical systems across the entire OT environment.

FortiAnalyzer offers centralized logging and reporting, centralized asset and network visualization, centralized event and incident management, and enables NOC and SOC analytics with support for hardware appliance or virtual machine (VM)-based deployments.

FortiManager provides centralized management and monitoring, security automation, and enterprise-ready integration with support for multitenancy and role-based administration, secure SD-WAN provisioning, and hardware appliance or VM-based deployments.

FortiSandbox provides AI-powered malware detection and response and automated breach protection with analysis that maps to the MITRE ATT&CK framework. It offers seamless integration with FortiGate and the Fortinet Security Fabric and supports ICS/OT applications and protocols. Standalone or centralized deployments and hardware appliance or VM-based deployments are supported.

FortiDeceptor uses a layer of decoys and lures to eliminate cyberthreats in their early stages. It emulates Windows, Linux, VPN, and ICS RTUs, and provides seamless integration with FortiGate and the Fortinet Security Fabric. It supports ICS and OT applications and protocols. Standalone or centralized deployments and hardware appliance or VM-based deployments are supported.

A Secure Foundation Ensures Business Continuity

For both OT and IT organizations, preparing for business continuity and disaster recovery is critical. When developing business continuity plans, organizations must ensure that they have the resources in place to secure a remote workforce and facilitate uninterrupted operations of OT and IT infrastructure both locally and remotely, while maintaining a good security posture.

Fortinet solutions are easily deployable and configurable so OT and IT organizations can maintain end-to-end security, visibility, and control for their digital assets regardless of their deployment environment.

[1] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 24, 2023.

www.fortinet.com

October 5, 2023 9:42 PM

950814-A-0-EN