WHITE PAPER

Leveraging FortiCare to Achieve the Highest Technical Operations

Service Offerings and How to Engage in Support

Executive Summary

As organizations continue to undergo digital innovation, it becomes increasingly important to have a security fabric that delivers broad visibility, integrated breach prevention, and automated operations and orchestration. To ensure organizations are getting the most out of their Fortinet investments, Fortinet Technical and Operational Support can help with architectural planning, diagnostics and troubleshooting, hardware replacement, efficient deployment, and overall achievement of the highest possible level of operations. This document will explain the available levels of FortiCare support, how to determine the best fit, the ticket process, and how to optimize support use.

Fortinet's custom-built hardware and proprietary OS means faster support resolution since no third parties need to be involved.

Support calls are answered in less than five minutes, 24 hours per day, seven days per week, 365 days per year.

The FortiCare Portfolio of Services

In the FortiCare portfolio, there are three functional areas: standard support, Advanced Services, and Professional Services. The standard support level is purchased by most customers for deployments of normal importance. Advanced and Professional Services are available for organizations that require faster ticket resolution or assistance in a number of areas such as planning, deployment, and training.

Foundational FortiCare Support Options

FortiCare services are available as per-device or account-based services. Per-device support is the foundation of support services and account-based services build on that foundation. These FortiCare services include an always-available technical resource 24 hours a day, 7 days a week, every day of the year. Either the 24x7 FortiCare service or Advanced Support Engineer (ASE) FortiCare service is purchased individually for each Fortinet unit placed into production. Both services provide firmware updates, technical support, and foundational FortiGuard subscriptions, as well as advance replacement. The advantage of ASE FortiCare is that it delivers faster ticket servicing turnaround.

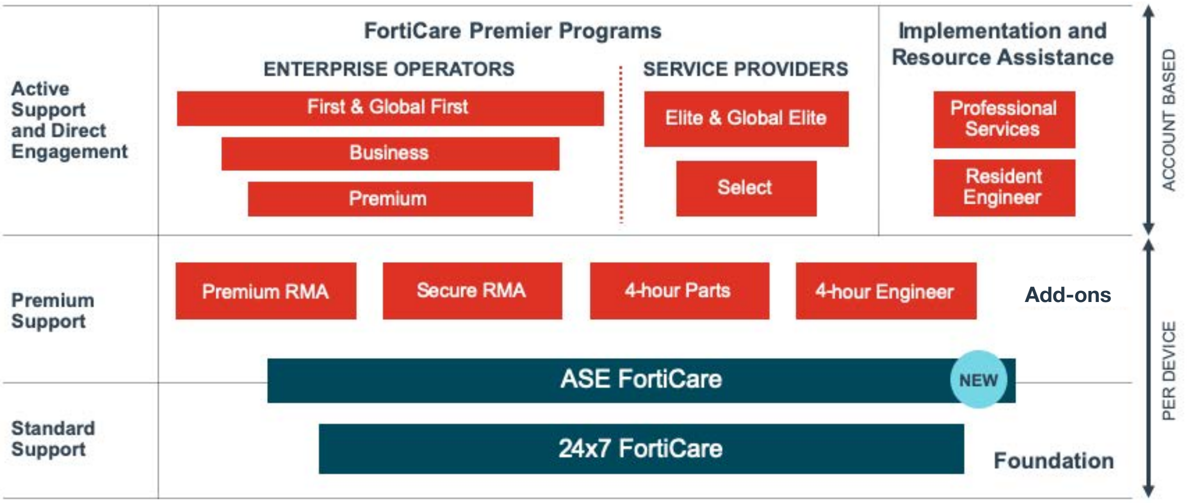

Figure 1: FortiCare services.

Account-based FortiCare services are selected once for the entire customer deployment or once per organizational unit in large enterprises. These services complement per-device services. A designated support engineer, logistics support, and training are provided. Account-based services fulfill specific design, implementation, and operation needs such as process alignment, compliance requirements, or complex integrations.

FortiCare services can be customized according to an organization's unique business needs, its tolerance for downtime, and whether a particular piece of hardware is protecting business-critical assets.

When to Choose ASE FortiCare

ASE FortiCare falls into the Advanced Services category and is ideal for the most sophisticated customers and complex deployments. The advantage of ASE FortiCare is that it provides the ability to reach the Advanced Services support team on a per-device basis, so efforts can be focused on the most important deployment areas. The following scenarios represent common situations that benefit from ASE FortiCare:

Reduced downtime

The cost of downtime is one way to determine if a particular deployment area (data center, remote office, network segment, etc.) is well-suited for ASE FortiCare support. Given that the ASE FortiCare support provides faster ticket response times and access to the Advanced Services team, customers experience an on-average reduced downtime.

Downtime has hard and soft costs. A hard cost is measured by the loss of ability to conduct a transaction with a customer. Soft costs are harder to measure, but can include loss of employee productivity, which can also be detrimental to business. With ASE FortiCare, organizations can see a return on investment (ROI) after just one ticket is fulfilled.

ASE FortiCare is recommended when a deployed Fortinet solution is protecting a top-tier critical business system or when the solution is necessary in order for more than 50 employees to perform their normal duties.

Business-to-business operations

Another situation that may require FortiCare ASE is when FortiGate is responsible for facilitating business-to-business (B2B) transactions. Increasingly, business sales and orders are handled between back-office systems and clients. These transactions can range from a simple email with an attached order, or they can be a more sophisticated application programming interface (API) transaction.

Regardless of how the systems communicate, they are critical to conducting sales and services transactions. Many of these systems can sustain small disruptions, but anything beyond a few minutes can have a substantial impact on the business and reputation. With training of Fortinet technologies, industry standards, and business continuity, the ASE FortiCare team can help keep business operations working and running smoothly.

Uptime of digitized processes

Organizations that heavily rely on digitized processes can also benefit from ASE FortiCare. The digitization systems rely upon the ability to communicate with each other and their control management system. ASE FortiCare reduces the severity and length of service impacts through priority access to the Advanced Services team.

FortiCare Premium Programs

FortiCare Premium Programs are account-based Advanced Services for larger organizations or those requiring specialized operational support. The offerings are broken into two segments: enterprise and service provider. Enterprises that leverage FortiCare Premium Programs are typically commercial or government entities that have established operational requirements, compliance objectives, and benefit from a programmatic approach to operations. Service providers that use the Fortinet Security Fabric for their internal operations are classified as an enterprise since the Fortinet components are not used for their service delivery. To be considered a service provider, managed services or managed security services using Fortinet technology must be delivered.

This support program is designed to deliver consistent services to customers through enabling their service-level agreements (SLAs), life-cycle maintenance, and recovery protocols. For enterprises, there are three levels to choose from that provide faster resolution and more access to expert help and guidance. For service providers, the service is centered around training the partner's delivery team and assisting with deployment logistics, as well as faster access to technical experts.

Many larger organizations, and those with complex deployments, prefer the vendor to provide a system of people and processes to align with their team. Organizations that have an established network operations center (NOC) and security operations center (SOC), compliance requirements, or newer deployments are most likely to benefit from account-based programs.

Benefits include:

- **Cross-ticket coordination and a cadence of reviews.** Cross-ticket coordination is important to organizations that have deployed many devices with similar hardware, firmware, and/or functions. The ability to access history across several tickets will help resolve similar situations faster and schedule preventative maintenance. Also, cross-ticket analysis is especially useful for service providers since their customers deploy common configurations, firmware, and network architecture. When a situation is discovered with one customer, the findings can be proactively applied to other deployments.
- **Training.** Each year, the customer's technical team can take NSE training courses and also the accompanying certification tests. This gives the team increased knowledge of the Security Fabric, which results in more stable device operations, better quality information for new tickets, and a more stable environment.
- **Service points.** Service points provide a flexible option to receive additional assistance from the FortiCare support team as needed through the year. Each account-based program provides a base number of points with additional points available for purchase. For example, a customer can use points to gain additional help from the support team with an upcoming maintenance window. Points can also be used in scenarios such as a firmware upgrade pre-test conducted in a Fortinet lab setting, a support account review at the customer's location, or for yearly planning sessions.

Fortinet representatives and Fortinet partners can help determine the best level of support for a given deployment scenario.

Fortinet Professional Services

Fortinet Professional Services consultants assist with the initial implementation and ongoing operation of Fortinet devices. These expert engineers are available for contract based upon custom-designed deliverables or three-month assignments. Professional Services expedite:

- **Technology migration** from one vendor to Fortinet
- **Initial implementation** and configuration services
- **Integration** of the Fortinet Security Fabric to other complementary technologies
- **Audits** including compliance checks or preparation for external auditors
- **Wireless implementation** for coverage tuning, performance enhancements, or adapting to changes in density needs or physical structures
- **Specialized product implementation**

FortiCare and Professional Services complement each other once the customer is in production. FortiCare assists with production systems experiencing technical difficulty. Professional Services consulting is a team of experts that implement, migrate, integrate, audit, and enhance Fortinet solutions. The devices and functions implemented by either Professional Services or the customer will be supported by FortiCare. As the customer and Professional Services engineers implement additional functionality, this increases the scope of how FortiCare can assist the customer.

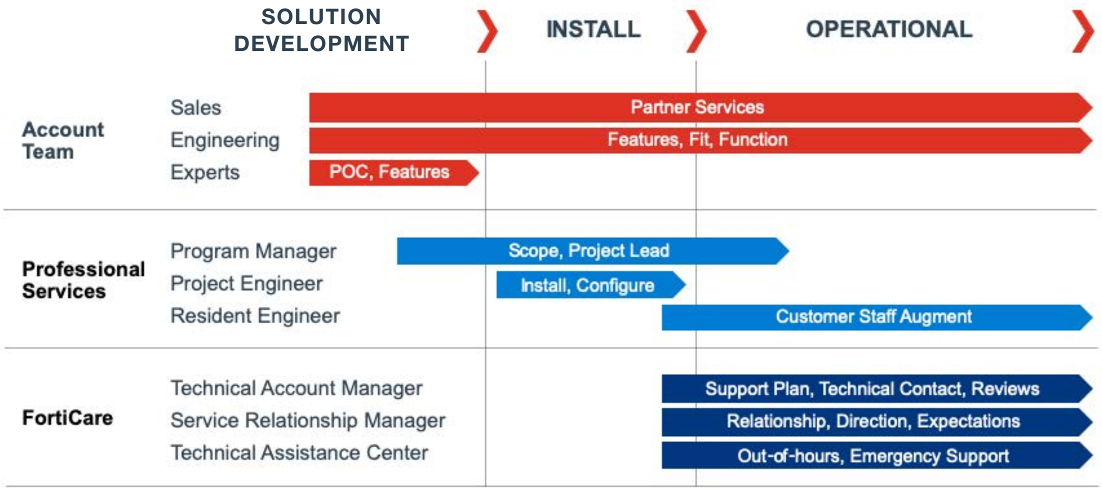

Figure 2: Fortinet Professional Services Engagement Timeline.

Hardware Device Replacement

The process of replacing hardware devices is called return materials authorization (RMA). The objective of this process is to replace hardware that has ceased to function correctly or as a last resort during the technical troubleshooting process. While Fortinet provides the highest hardware device quality, sometimes environmental conditions and individual component failures require that a unit be replaced.

Advance Replacement

All FortiCare per-device contracts come with the Advance Replacement hardware service. This service ships a replacement hardware unit to the customer before they must return their faulty unit from their production environment. The replacement is sent to arrive the next business day after technical confirmation of a hardware issue by a Fortinet support engineer. The RMA process is tracked through a FortiCare ticket that includes the background information, the required FortiCare RMA authorization, shipping address, tracking information, and more.

Once the customer receives the replacement device, they have 30 calendar days to ship the original, replaced device to Fortinet. A return address will be provided in the FortiCare RMA ticket. It is the customer's responsibility to provide the shipping label. The box in which the replacement device was shipped should be used as the container for sending back the original unit. This is important as the box will have the necessary padding and plastic covers to keep the unit from becoming damaged.

It is important to keep the FortiCare Support Portal updated with accurate information so there is no delay during the RMA process. It is key to maintain the following:

- An active FortiCare support contract for the device
- A common name or description on the device to easily locate it in the portal
- The physical location of the device

Premium RMA

The Premium RMA support level is for customers who require faster hardware replacement than the Advance Replacement level. Advantages include:

- **Country import controls.** In some geographical regions, a customer's country will have import controls for the country in which the replacement hardware is stored. Premium RMA pre-allocates a hardware spare to be located within the customer's country to incur the import controls ahead of when the device is needed. This setup provides immediate shipping from the hardware warehouse to the customer's site using normal shipping methods that don't require import controls.
- **Next-day delivery.** The Advance Replacement next business day service does not provide shipping over established holidays and weekends. This can result in a replacement device taking several days longer to arrive at the customer's location. Premium RMA uses next-day delivery, providing shipping and delivery on holidays and weekends.
- **Expedited delivery.** For customers needing devices within four hours, some geographical regions have a four-hour delivery option. This is common for many customers who elect to not purchase redundant devices, cannot rack or store cold spares, or need to align with other recovery procedures.
- **Physical device replacement assistance.** In combination with the expedited four-hour delivery above, an equipment engineer will arrive in parallel to the device, providing physical replacement assistance. The engineer will swap the current production device with the replacement hardware unit provided (including power and data cables), install the customer-specified firmware level, and configure the device for network management access.

FortiCare Support User Guide

The following explains how to use FortiCare services to achieve the best outcome whether there is an urgent, top-priority issue, or guidance is needed for a new project. To engage with FortiCare support, the first step is to create a ticket. The FortiCare technical support ticket is the main conduit of information sharing between the customer and the assigned support engineer. Everything that the support engineer knows about the deployment, device's state of operation, etc., is learned through the ticket or verbally over the phone. The ticket enables data uploads to be transferred to provide extremely valuable insight into the current and historical operation of the device.

Entitlement Registration Process

A device's support entitlement for Fortinet FortiCare Technical Support services is enabled by a FortiCare contract. After purchase, a PDF document will be sent to the device's owner that contains the information necessary to register the contract with FortiCare systems. One support contract is applied to one device (a 1:1 relationship). FortiCare support services (technical support, firmware, etc.) will not be available for the device until a valid FortiCare contract has been associated with that device.

Support Ticket Guidelines

This section covers who should open tickets and what is required before and during the ticket creation process.

Qualifications to open support tickets

All operations personnel meeting the following requirements may open a ticket:

- The person opening the ticket must have rights according to their Fortinet Support Portal credentials. This applies to tickets opened through the Support Portal and also through the phone service.
- The person opening the ticket must be able to provide the required information and initial diagnostic dataset to kick-start the technical investigation process.

What to do before opening a ticket

If the situation is urgent (complete or partial outage), a ticket should be opened immediately with supporting information and then immediately phone support. If not, before opening a ticket, the following steps should be taken:

- Look at the recent configuration changes to determine if a misconfiguration is causing the undesired change. All changes should have a predetermined rollback mechanism, even if it is simply to roll back to the most recent configuration.
- Consult the documentation for other configuration parameters. This is available through the device's console or terminal interface. This can often tweak the system's operation to resolve a dependency or integration incompatibility.
- Cross-test or triangulate the error by attempting to reproduce the error on several machines to validate the likelihood of the Fortinet device causing the situation. This information may help identify how to resolve the situation or be helpful to include in the ticket.
- Consult Fortinet Cookbooks to see if detailed instructions are available for your scenario, as they might include configuration and testing tips. Cookbooks can be found with FortiGate documentation.
- Search the Fortinet Knowledge Base site. Most FortiCare tickets are either resolved or follow a Knowledge Base article through the technical issue identification and resolution phases. A quick search on this site can provide ideas on additional areas to investigate ahead of opening a ticket. Or it may provide additional pieces of information that will help the ticket be resolved sooner.

If these steps have not helped resolve the issue, open a FortiCare technical support ticket.

Detailed steps for opening a FortiCare Technical Support ticket are available on the Support Portal: https://support.fortinet.com/Information/DocumentList.aspx in a document titled Ticket Creation Guide.

Information that must be included in a ticket

For faster resolution, customers should provide detailed historical data files in addition to the short problem summary when creating a ticket. The following information is needed when a ticket is opened. Some information may need to be provided as attachments.

- **The current configuration of the device.** This is critical since the support engineer needs to know how the device is configured to locate possible misconfigurations, test scenarios in the FortiLab, and cross-check narrative descriptions in the ticket to lines within the configuration.
- **The last known good configuration.** If a configuration was recently made to the device, it is extremely helpful to have a configuration file from when the environment was operating as experienced. This last-known good file can be from 24 hours or even a month previous. The goal is to have a working point of reference during the analysis process.
- **The correct firmware version.** When the ticket is created, there is a section to identify the currently running firmware or software version. This information is used in conjunction with the provided configuration. It is also important to know if the firmware or software version was recently changed, so the support engineer has accurate information when reviewing historical information.

- **TAC report.** The Technical Assistance Center (TAC) report comes from the Fortinet device and provides a complete set of diagnostic data in a single file. The TAC report is accessible from the browser HTTPS interface and also the console (or command line system access through SSH or other means). The TAC report is a 5–15 MB ZIP file. The file is easiest to obtain through the graphical user interface (GUI) or HTTPS interface. The same data can also be captured live from the device's console and placed into a plain text file.
- **Relevant device logs.** The last 48 hours of device logs should be searched and relevant logs should be attached. Fortinet recommends sending device operation logs that show configuration changes, any device operation notes, and system changes. Depending on the technical need, it might help to send functional logs such as VPN, IPS, web content filtering, etc.
- **Network diagram.** Even a basic network diagram is helpful when attempting to visualize the flow of traffic from the source through the Fortinet device to the target.
- **Primary and secondary points of contact.** A primary and secondary point of contact are required. This is especially important if the operation is global or if it is a top-priority case. FortiCare engineers can only work with authorized contacts. The owner of the account configures the authorized contacts through the Support Portal by specifying their names, phone numbers, and email addresses. Only the persons identified on the support account can be assisted. Please note that callback numbers provided in the ticket do not have to be preregistered. It is important that there is always a technical operations contact available to answer a callback from a Fortinet FortiCare support engineer.

Ticket Priority Levels

The FortiCare Service works with a categorization system that is used across all ticketing systems, phone calls, and management review meetings, and within the service description with the assignment of resources. Fortinet designates priority levels to communicate how seriously the customer is impacted by the reported issue. Priority levels range from level 1 through level 4. These are often shortened to P1, P2, P3, or P4 when using the Fortinet portal system or other documentation.

- **Priority 4 (P4).** P4 tickets are noncritical situations and track general requests. This is the least concerning level. It represents something that is not time-sensitive and has a negligible impact on the device's operation. Often, P4 tickets are those awaiting final confirmation from a customer who has applied the solution and confirmed that the technical issue has not been noticed again by users. In addition, P4 can represent an account management need regarding the registration of a device, changing ownership of a device, correcting erroneous data in the Support Portal, and other account management needs. This is also the level identifier that is used when customers have sent a new feature request for a particular device.
- **Priority 3 (P3).** P3 is where most tickets start and Fortinet support engineering resources are engaged to assist the customer in the technical resolution. This represents the first level for a ticket that is impacting a customer's operation. Most tickets are initially assigned this priority level as initial data is being gathered and impact severity is being assessed. This also represents the highest level that a customer can request when opening a new ticket on the Support Portal.

  In general, P3 tickets represent situations where a technical issue has been identified, yet the particular function of the device is still operating, at least in part. This may result in slow function or inconsistent behavior. Many P3 tickets should be moved to P2 status, but insufficient data is available. Often missing are diagnostic data, interactive troubleshooting data output, and/or a detailed description on the impact and experienced behavior.
- **Priority 2 (P2).** P2 tickets are situations where the impact to the customer's operation has been confirmed. In this scenario, Fortinet resources work to resolve the technical issue with one or more (but not all) functions of the device, and the associated user/system activity has been isolated. This level represents a partial outage being experienced as a result of an identified technical fault. A partial outage is where a particular function of the device is not operating, resulting in services or users not being able to accomplish a particular task. Some examples of functions include SSL VPN, mail quarantine, and offline security inspection.

  P2 requires that the technical issue be identified and reproducible. In these cases, the issue has been identified and the team can assign resources to determine how to resolve the situation. A P2 ticket can also represent a significant risk identified by the customer or Fortinet to the current device's operation. These are situations where the risk has not yet impacted operations and is usually discovered by advanced users within the customer's organization or through functional testing. While these discoveries are often resolved through an adjustment of configuration, sometimes deeper diagnostics and controlled testing are required to get at the root of the problem.
- **Priority 1 (P1).** P1 tickets are a verified complete outage where the device is not passing traffic or where administrative access is not possible by any method. This is the highest level possible for a FortiCare technical support ticket. While this ticket level is rare, it is assigned when the customer is experiencing a complete outage of their device for all functions or it is unable to be managed. Normally, these situations result in the complete stoppage of traffic flowing through the device. It could be that the Fortinet device did not respond in an expected way to another failure in the environment, resulting in the overall environment to not pass traffic as necessary for users and systems to communicate.

P1 is also assigned when the ability to manage the device is lost. Secure, consistent, authoritative access to devices is fundamental. A complete loss of management through FortiManager, all IP-based access methods, and the physically connected serial console cable (provided in the original packaging) are required to receive P1.

P1 is also assigned when a known good device configuration is applied but it does not change the device's operation behavior. This scenario can stem from an underlying condition that needs to be addressed immediately.

ASE FortiCare Escalation Process

Sometimes there is miscommunication or the importance of the situation has not come across in the standard ticket communication. This is why Fortinet provides an escalation process for when a situation arises that requires more attention.

The FortiCare service level can be increased any time to meet changing operational needs.

Before starting the escalation process, check the following list:

- Verify that all relevant information has been provided in the ticket and communicated to Fortinet support.
- Clearly document in the ticket the increased business impact or extended deadlines caused by the incident.
- Inform your management of the situation and make sure they are available to engage if necessary.
- Designate the appropriate level and availability of technical resources within your organization that are available to work with technical support. This is key as the customer's assistance will be required immediately for P1 incidents.

After completing the list items above (if necessary):

- Call the global support number and ask for the assigned engineer. Since the assigned support engineer already has the most knowledge about the situation, it is best to work directly with them to understand what is currently being investigated. If the assigned engineer is not available, the shift manager will be able to determine how to proceed.
- After speaking to the engineer, start the escalation process.
  - Be ready to provide the ticket number.
  - Telephone the FortiCare Technical Support Center.
  - Provide the customer service representative with the ticket number and request to talk with the duty manager for an escalation. The customer service representative will then transfer you to the duty manager.

FortiCare management will have to assess the situation before determining how to accelerate the resolution time. Further, the request for a ticket escalation does not guarantee that the priority of the ticket will be increased.

Additional information is available in the FortiCompanion for Technical Support document that is located in the FortiCare Support Portal.

Guidelines for Using the FortiCare Ticketing System

By design, a ticket will change priority levels from the time that it is opened until it is closed. Ticket levels are changed by the assigned FortiCare support engineer or support management. The current priority status is available in the FortiCare Support Portal or via the assigned engineer. The same support engineer often stays assigned to the ticket even though the priority level has been adjusted. Ticket priority levels are changed to reflect the current status of the situation.

The following are important things to know when using the FortiCare ticketing system.

- **All communications must be in the ticket.** The support ticket is the record-keeper of all interactions between Fortinet and the operator(s) assisting with the resolution. Keeping all communication in the ticket is required to keep all parties informed. Tickets are used by Fortinet when additional engineers come to assist, when one regional team passes off to another region, when a new support engineer is assigned, and when escalation is needed, to name a few examples. For communication that happens outside the ticket, such as phone calls and interactive sessions, the activity should be summarized in the ticket with clear next steps and assigned owners.
- **Tickets will close if no response is received.** Fortinet monitors tickets that need a response from the customer either for requested information or validation that a problem has been solved. After working through a problem together, the customer's confirmation that the situation has been resolved enables Fortinet to mark the ticket correctly for better personnel training and updating our knowledge

system with verified solutions. If a customer has not replied to a ticket, the Fortinet ticket system will auto-close the ticket. When additional assistance is still needed for an auto-closed ticket, another ticket will be created with a reference to the original. We kindly ask customers to update the support ticket each week to inform us of their progress.

- **It is the customer's responsibility to make changes.** Through the support ticket, Fortinet will recommend changes after receiving enough diagnostic information. Making the recommended changes and gathering the diagnostic information are the responsibility of the customer (or someone authorized by the customer). The customer must evaluate the impact of the commands on a device that is in production. Fortinet recommends that customers attend sufficient training to: understand the console commands, navigate the GUI, and follow their organization's internal processes for change.
- **Device registration is required for FortiCare support services.** FortiCare support contracts are tracked per device serial number. The serial number is a unique identifier created for hardware, virtual machines, and software sold by Fortinet and operated by customers. When FortiCare is purchased, an entitlement PDF is provided that contains the contract entitlement number used to register the contract on the FortiCare Support Portal. During the registration process, the support contract is tied to a serial number. All subsequent technical support tickets, firmware downloads, and FortiGuard Application Control subscription update services are enabled based upon the level and duration of the contract. FortiCare support services cannot be delivered for devices that do not have a valid support contract.

Fortinet offers an Enterprise Agreement that enables customers to purchase sitewide coverage for FortiCare (Enterprise Support Agreement) and FortiGuard (Enterprise License Agreement) entitlements.

- **FortiCare welcomes partner assistance.** Fortinet sales partners are important throughout the customer's journey. Customers may authorize a partner to contact Fortinet on their behalf. Partners are often provided with account access on the Support Portal through subaccounts.

Global Coverage for FortiCare Customers

Fortinet FortiCare technical support operations provide global support services for our customers around the world. FortiCare is present in three major regions: North America, Europe, and Asia Pacific. Technical Assistance Centers provide around-the-clock technical aid for deployed devices, whether the customer is located in a particular country or has deployments throughout the world.

The address of a given device will determine which Technical Assistance Center and hardware replacement warehouse it is automatically assigned to. It is critically important that customers keep the registered address for each device up to date to ensure the best technical ticket routing and hardware replacement shipping speed.

Fortinet has a global follow-the-sun operations model. All inbound support calls are routed by the customer service desk to the region that operates during the area's normal business hours. This means that a customer calling during their evening will be routed to a FortiCare Technical Assistance Center in another region for support. This is best for customers since FortiCare support engineers will be available to assist with their technical needs.

P3 and P4 severity level tickets are handled in the region in which they are originally assigned. Fortinet strives to keep the ticket assigned to the same Technical Assistance Center and the same engineer whenever possible for consistency and faster resolution.

For P1 and P2 severity tickets, the initial assignment when a ticket is created will be to the currently active FortiCare support region. Tickets of this severity may be reviewed by several engineers, and the support shift manager will coordinate additional resources to assist. P1 and P2 tickets are commonly given to the next active Fortinet Technical Assistance Center during follow-the-sun transitions (at the conclusion of each region's business hours). Please note that tickets are handed between similar teams; for example, standard FortiCare and Advanced Services FortiCare (the latter includes ASE FortiCare).

Maintaining Device Access for Troubleshooting

FortiManager and FortiAnalyzer

As key components of the Fortinet Security Fabric, management appliances or virtual machines are available to assist customer operations across multiple deployments, manage access for multiple administrators, retain longer records of management activity, or implement additional procedural controls. These management systems communicate directly and securely to the Fortinet device using an API. These management components are key to troubleshooting and it is important to:

- Maintain access to FortiManager and/or FortiAnalyzer at all times. The historical data in these systems can assist in the information gathering for diagnostics.
- Regularly check to make sure FortiManager and/or FortiAnalyzer is/are collecting the expected data such as log files, configuration changes, etc.

Web-based GUI

All Fortinet Security Fabric devices have a web-based GUI. This access is secured through SSL encryption and guarded by required user credentials (username, password, and optionally FortiToken). This administrative access method requires less user knowledge of the system than SSH or console access, since a computer mouse is used to navigate graphical icons. Not only is the GUI a unique access methodology for troubleshooting but it also provides advantages including:

- Less user training is required to access the GUI, so troubleshooting can begin at a faster pace with less detail.
- Granular permission levels can be set on the GUI so that all operators can view important information (but not make changes).
- The GUI access method uses standard HTTPS that will provide wider access compared to SSH and console.

Secure shell (SSH)

Secure shell (SSH) is an encrypted text communication between an operator and the operating unit. Most desktop operating systems have a built-in or free client that makes this management access method very popular. This IP-based console access provides the richest access to the device's operating configuration and diagnostic tools available. Most troubleshooting processes will involve troubleshooting commands that will take place on the device's console, normally accessed through SSH. It is important to regularly test SSH access to the device using directory credentials (RADIUS, LDAP, etc.) and local credentials (username and password stored locally on the device).

Console cable

A serial console cable is a physical connection to the physical operating unit. All physical Fortinet units provide a serial console access method, no matter the form-factor size. Console cable connections are DB-9, Cat5 Ethernet, or USB. All of the physical connection form factors provide an extremely simple management access methodology that is stable and is a necessary backup option. Further, Fortinet software will provide output in text form to the console port during normal, abnormal, and startup operation. These messages cannot be retrieved in any other way. Console access is mandatory during the troubleshooting process when:

- Management access cannot be gained through the device's management IP interface
- Boot-time text readouts are necessary for diagnostics
- A hardware test may be required through using dedicated HQIP firmware.
- System readout information cannot be gained through the normal system logs

There are many solutions available that provide access to the console connection port over IP for remote access. These solutions provide an SSH connection to the operator and then convert the commands and text to the serial console connection. These are very valuable since they retain the various console log messages, giving unique insight into the conditions surrounding the first fault.

Hypervisor access

If the deployed device is running on a hypervisor, maintaining console access at all times during its operation is critical. Since a physical console serial cable cannot be connected to the device as a last resort, the hypervisor system provides the most rudimentary access method. Console access via the hypervisor using local credentials (not RADIUS, LDAP) should be regularly tested. Some public cloud systems do not provide a serial console access method. In this case, it is recommended to have a logically close access host to manage the device. This removes any complications of routing, security policy, network congestion, etc.

How to Register a Device

- Go to https://support.fortinet.com.
- Log in using your preregistered user account.
  - If you do not have an account, click the REGISTER button.
- Select Asset > Register/Activate.
- In the Specify Registration Code section, enter your product serial number, service contract registration code, or license certificate number to start the registration.
- In the End User Type section, select either Government or Non-Government user.
- In the Product Description field, enter a comment as to where this unit is physically located.
- Select the appropriate Fortinet Partner.
- Select Next.
- Select the checkbox indicating that you have read, understood, and accepted the Fortinet Product Registration Agreement (EULA).
- Select Next.
- Select the checkbox indicating that you are activating the support contract and agree to the entitlement period. Once accepted, the entitlement period cannot be changed.
- Select Confirm.

Note: For bulk registrations of multiple serial numbers, please email cs@fortinet.com (and copy your TAM if you have an Enterprise or Service Provider Advanced Services contract).

Firmware Updates Are Important

Firmware and software updates integrate fixes discovered through continual testing and analysis of challenges noticed in field deployments. Since firmware patches incorporate these fixes, they help customers minimize technical problems that have been resolved through additional development. Customers have the opportunity to update their field devices through the Support Portal and should do so regularly throughout the year. Firmware should be updated twice per year.

This maintenance cadence can also eliminate the need to update the firmware as an initial step in the troubleshooting process. Since Fortinet invests heavily in continual firmware and software development, this is a critical component of the troubleshooting process. Please expect that some situations require that customers apply more recent firmware to proceed in the diagnostic process.

Technical Operations Checklist: How to Achieve the Best Possible Level with Fortinet

There are a number of variables that contribute to the success of technical operations, and there is no one right way to do things that fits every organization. There are consistencies across organizations, however, that can provide guidance during the decision-making process and keep things running smoothly. The following contribute to successful operations:

Training. Fortinet's global training program is where all operations planning should start. Knowledge and skills using Fortinet products are fundamental to handling technical operations. Fortinet strives to make the vast capabilities of the Security Fabric accessible to all users, yet the complexities that come with operations are managed through training knowledge. Fortinet provides free and paid training programs delivered online (self-led and instructor-led) and also face-to-face classes. Further, Fortinet includes training in the higher-level FortiCare services.

Professional Services. The technical design phase of a new solution or change to an existing deployment needs to include the availability and capability of an organization's resources to carry out the change. Fortinet Professional Services provides temporary or longer-term technical experts to assist with successful implementation, integration, migration, and other enhancements to business systems. Reliable solutions start with the correct implementation. For instance, engaging Professional Services can expand the implementation to accommodate planned changes for scalability, compliance, business organizational changes, and more. By anticipating and addressing these changes, there is less impact on the production system when business requirements change.

The right FortiCare service level(s). It is important to choose the right service level for your organization's needs. The level of Fortinet FortiCare can be adjusted over time, so it is a good idea to reevaluate what is needed every six months. Not selecting the FortiCare service level that fits the organization's needs can result in a misalignment between the FortiCare team and the customer's operations team, resulting in difficult problem resolution.

Intelligent change. The majority of tickets received by FortiCare are technical problems resulting from a change to an environment that was previously stable. Every organization should have a change control process. For some, this will be a formal process involving a change approval board and require prevalidation in a testing lab (including change rollback protocol). For others, it will focus on cross-department communication and scheduling.

Solution lab testing. Lab testing should be present in all organizations since it provides the ability to refine changes in a safe environment and fosters learning. Organizations should strive to create a lab environment that mimics their production environment, or at least the critical functions. By testing changes in a lab environment, disruptions to production systems will be reduced, lessening hard costs to the business. Lab testing will also enable firms to refine the change to be made, resulting in a quicker implementation. Plus, it will help determine whether the change was successful or not. Fortinet provides discounted devices to help customers build their lab successfully.

Dynamic configurations. Fortinet technologies can be set to adjust policy or controls based upon changing variables. This style of implementation provides the ability to dynamically adjust the effective policy through modifying external systems or natural conditions. The result is fewer configuration changes to the production system, resulting in more stable operations. Fortinet also includes the ability to categorically set policies rather than explicit conditions. A good example is web content filtering where an entire category can be blocked (e.g., sports, movies, etc.), instead of adding individual websites to be denied. This approach will result in less effort to maintain the environment and fewer changes.

Availability and performance monitoring. Operations monitoring provides the data needed to understand how the system is working and when something needs attention. These recommendations are for operations monitoring and do not cover security monitoring:

- **A baseline of operations.** Fundamentally understanding how a device is operating is the first step in operations monitoring. It is important to have this information before a technical fault occurs in the environment, so there is a baseline to which the current operation can be compared.
- **Diagnostic output.** Fortinet technology provides diagnostic data during system events. Some of this data is retained in permanent messages like Syslog but others (sometimes the missing puzzle piece) are only captured if monitoring is set up in advance.
- **Individual component monitoring.** User traffic, computer systems, and application systems include many different types of traffic such as DNS, HTTP, HTTPS, NTP, and more. Traffic types have different destinations as well: local network, data center, cloud, and internet, for example. These communications become a multidimensional web that can be broken down into individual components. Two key takeaways are that some faults progress in severity, so it is possible to spot a technical fault before it has a production impact. And, when a user or system is impacted, it is critical to understand exactly how with enough detail to create a scientific description.
- **Dependency monitoring.** Fortinet technology relies upon other systems to operate. Knowing the availability and performance of these other resources will help in identifying a secondary issue on the Fortinet device. Examples of resources that can affect Fortinet devices are the electricity source and the Microsoft Windows Activity Directory connection. Mapping these dependencies and putting monitoring in place will assist in faster diagnostics and resolution.

Maintenance routines. Implementing consistent routines can prevent problems that could impact operations. Maintenance of technology platforms must be balanced with the change that they introduce into an environment. For highly sensitive operations, Fortinet Professional Services should be engaged to create a customized program. Required maintenance for smooth operations include:

- **Firmware updates.** Fortinet recommends firmware patches (incremental software updates with fixes) be applied twice per year and a change to a newer major release every two years. For example, a device would upgrade to 6.0.3 and 6.0.5 the first year and then 6.0.7 and 6.2.3 the following year.

- **Hardware diagnostics.** All Fortinet hardware includes diagnostic features that run either on an automatic schedule or upon an event like a reboot, and when manually invoked. A device's operation environment and physical characteristics must be considered to determine an appropriate schedule, which can be no less than once per year. A maintenance window or low production time will be required. It is highly recommended that any relevant hardware tests are performed before a major configuration change or firmware update is started. Recommendations include: reboot the device to invoke bootstrap testing, test hard drive consistency, search logs for system events, and search console notices.
- **High-availability testing.** High-availability clusters are critical for continuity of operations when the cluster notices a fault. While there are many forms of clustering, each has means to validate the state of the cluster and readiness for a transition. It is recommended to check these metrics every three months or implement monitoring that can automatically alert on unexpected changes. In highly sensitive operations, customers might also elect to conduct failover and failback tests to validate that neighboring network switches and network routing recover correctly.
- **Subscription entitlement.** For customers using the Security Fabric with FortiGuard subscriptions, there are two macro elements to audit. First, the entitlement contract end date must be tracked to renew before the subscriptions expire. In large environments, FortiManager is helpful since a report is available with the information. Second, auditing the logs (or setting up an automated notification through FortiAnalyzer, FortiSIEM, or other log management system) for failed attempts to download the latest subscription package or the inability for the device to reach the FortiGuard distribution network. Either of these events causes the configured security policies to be ineffective, less effective, or inconsistent.
- **Verification of local admin access.** Local admin access is critical for some diagnostic and recovery situations. Every three to six months, local administrative access (administrative credentials not requiring external directory services such as LDAP, RADIUS) should be tested.

Partner with Fortinet FortiCare for Smooth Technical Operations

FortiCare provides flexible support and operational offerings to help companies accomplish their initial and ongoing objectives. FortiCare services support the entire Fortinet Security Fabric, making available a single source for troubleshooting and resolution of any issues that may arise. FortiCare Technical Support services, coupled with architecture and deployment support from Fortinet Professional Services, help organizations reach security and operational efficiency goals quickly and maintain smooth operations.

www.fortinet.com