**What does the FortiGate basic functionality include?**

Each FortiGate hardware provides the following basic functionality:

|  |  |
| --- | --- |
| Fortinet VPN | **Virtual Private Network (VPN)**  Fortinet offers basic VPN functionality, either as hardware through FortiGate appliances or as software through FortiClient. For example, two FortiGates (or standard-compliant third-party devices) can be used to securely connect multiple sites via a VPN network. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/b8b38b2997414996b46bb639a46c3313) |
| Fortinet SD-WAN Services | **SD-WAN Services**  SD-WAN is a way to manage a large number of connections and dynamically route traffic over the best available connection. SD-WAN provides redundancy as well as more capacity with multiple Internet connections. SD-WAN solutions are significantly less expensive overall than MPLS, considering the time of installation as well as deployment. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/2efb02dc8b224942a7f2d2a2fbe35abb) |
| Fortinet Applikationskontrolle | **Application control**  There are more and more applications that rely on web services and make life hell for administrators in terms of security. Therefore, it is becoming increasingly important to work granularly in order to guarantee performance, speed, reliability and, above all, security. One example is the third-party use of protocols that can be tunneled, for example, and are thus separated from the application traffic. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/57bcf91c8c6448a4ae5d587f388fec47) |
| Fortinet FortiCare Support | **FortiCare Support**  Fortinet's team of experts is available around the clock to help with problems and handle tickets promptly. However, through FortiCare, you also get important firmware updates on your Fortinet devices. There is a pre-replacement service which, in the case of defective devices, sends you a replacement device immediately after the RMA ticket has been approved. This means that the defective device does not have to be sent to Fortinet beforehand. Please note that without a license you can only use FortiCare Support for 90 days. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/146e1e2ef170445ba5ef331501e90b9a) |

**What does Fortinet Advanced Threat Protection include?**

Fortinet Advanced Threat Protection (ATP) provides the following features in addition to the basic functionality of each FortiGate:

|  |  |
| --- | --- |
| Fortinet Antivirus | **Antivirus**  Fortinet's optimized anti-virus technology uses machine learning to provide multi-layered, real-time protection against multiple forms of attack. It is able to detect known virus signatures, but also to identify modified and completely new virus variants through grayware scans. Fortinet provides a spectrum of known viruses to streamline the process of virus analysis. Part of Fortinet Advanced Malware Protection (APM). [More informations ❯❯](https://www.enbitcon.com/widgets/cms/3a5ff75f0e84486f8bdeabf6037358de) |
| Fortinet Intrusion Prevention System | **Intrusion Prevention System (IPS)**  Intrusion prevention systems provide protection against known and future threats at the network level. In addition to signature-based detection, anomaly-based detection is performed. The system sounds an alarm when data matches a specific profile of attack behavior. In combination with FortiManager and FortiAnalyzer, even highly complex VPN infrastructures can be implemented in a flexible, simple, cost-effective and multi-tenant manner. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/9f0f38269dac48d0b80edf9962254d34) |
| Fortinet Mobile Security | **Mobile Security**  The drastic increase in mobile devices, some of which are also the private property of the user, presents companies with a new challenge: control over devices to which, due to the legal situation, no or only very limited and, above all, regulated access is possible. Fortinet Mobile Security uses special parameters to detect the end devices (type & manufacturer) and the installed operating systems (type & release). Part of Fortinet Advanced Malware Protection (APM). [More informations❯❯](https://www.enbitcon.com/widgets/cms/39f33455cbbc4b38a4da63af336e10ad) |
| Fortinet FortiSandbox Cloud | **FortiSandbox Cloud**  The powerful cloud-based FortiSandbox enables enterprises and government agencies to detect and prevent high-threat attacks such as advanced persistent threats (APTs) more reliably than ever before. It is typically at the end of the line of many security mechanisms in an IT infrastructure and it can take a good few minutes for threats to be released or destroyed. Part of Fortinet Advanced Malware Protection (APM). [More informations ❯❯](https://www.enbitcon.com/widgets/cms/57bcf91c8c6448a4ae5d587f388fec47) |

**What does Fortinet Unified Threat Protection include?**

Fortinet Unified Threat Protection (UTP) provides the following features to complement Fortinet ATP:

|  |  |
| --- | --- |
| Fortinet Anti-Spam | **Antispam**  Fortinet's antispam technology provides comprehensive capabilities to identify and block spam mails. Similarly, malicious email attachments are reliably detected to fend off attacks from spam bots and compromised systems. FortiGate and FortiWiFi platforms offer built-in anti-spam functionality as part of their multi-layer protection mechanisms. These are kept up-to-date through regular FortiGuard updates. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/1ec047badfb24a4c81c69f97a5b1271a) |
| Fortinet Web Filter | **Web Filter**  Unauthorized Internet surfing and use of web-based applications often result in lost productivity, high network load, malware infection and data loss. URL filtering, content filtering and the FortiGuard Web Filter Service can ensure that no one is anywhere they shouldn't be. At the same time, your own network is kept safe by blocking relevant content. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/05d8a6d1ae344d54adb9c29668c16dae) |

**What does Fortinet Enterprise Protection include?**

Fortinet Enterprise Protection offers the following features in addition to Fortinet UTP:

|  |  |
| --- | --- |
| Fortinet Industrial Security Service | **Industrial Security**  The Industrial Security Service protects the ICS and SCADA area of the enterprise OT by blocking or restricting access to risky system protocols. It also provides security and control for over 100 industrial applications. Through the Industrial Security Service, you get real-time updates to fight cyber-attacks. It supports the main ICS manufacturers to secure your vulnerabilities. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/741bccbf87ae413694a12373f982a605) |
| Fortinet IoT Services | **IoT Detection**  The IoT Detection Service helps customers significantly reduce their attack footprint by enabling the Fortinet Security Fabric to automatically detect, segment and enforce policies against IoT devices based on FortiGuard intelligence. With this service, FortiGates can query FortiGuard servers to get info über unknown devices and then act accordingly based on policies. [More informtaions ❯❯](https://www.enbitcon.com/widgets/cms/4bcba7ea78d348389f730dc165775ce0) |
| Fortinet FortiConverter Service | **FortiConverter**  Migrating old, complex device configurations to new next-generation solutions can be a major challenge and take a lot of time. Often, some mistakes are also made during this process. With FortiConverter, you can enable a smooth migration while automatically eliminating errors and duplicate information. This will save you time and effort. [More informations ❯❯](https://www.enbitcon.com/widgets/cms/ef5cca7d8695496c817b6f27ce2a1a59) |
| Fortinet Security Rating Service | **Security Rating Service**  The Security Rating Service improves and facilitates network configuration, provisioning of new hardware and software, and more visibility and control over the network. Regular monitoring by the Security Rating Service increases network security over time. By performing audit reviews, security teams can identify vulnerabilities and configuration weaknesses in their security fabric and implement best practice recommendations. |