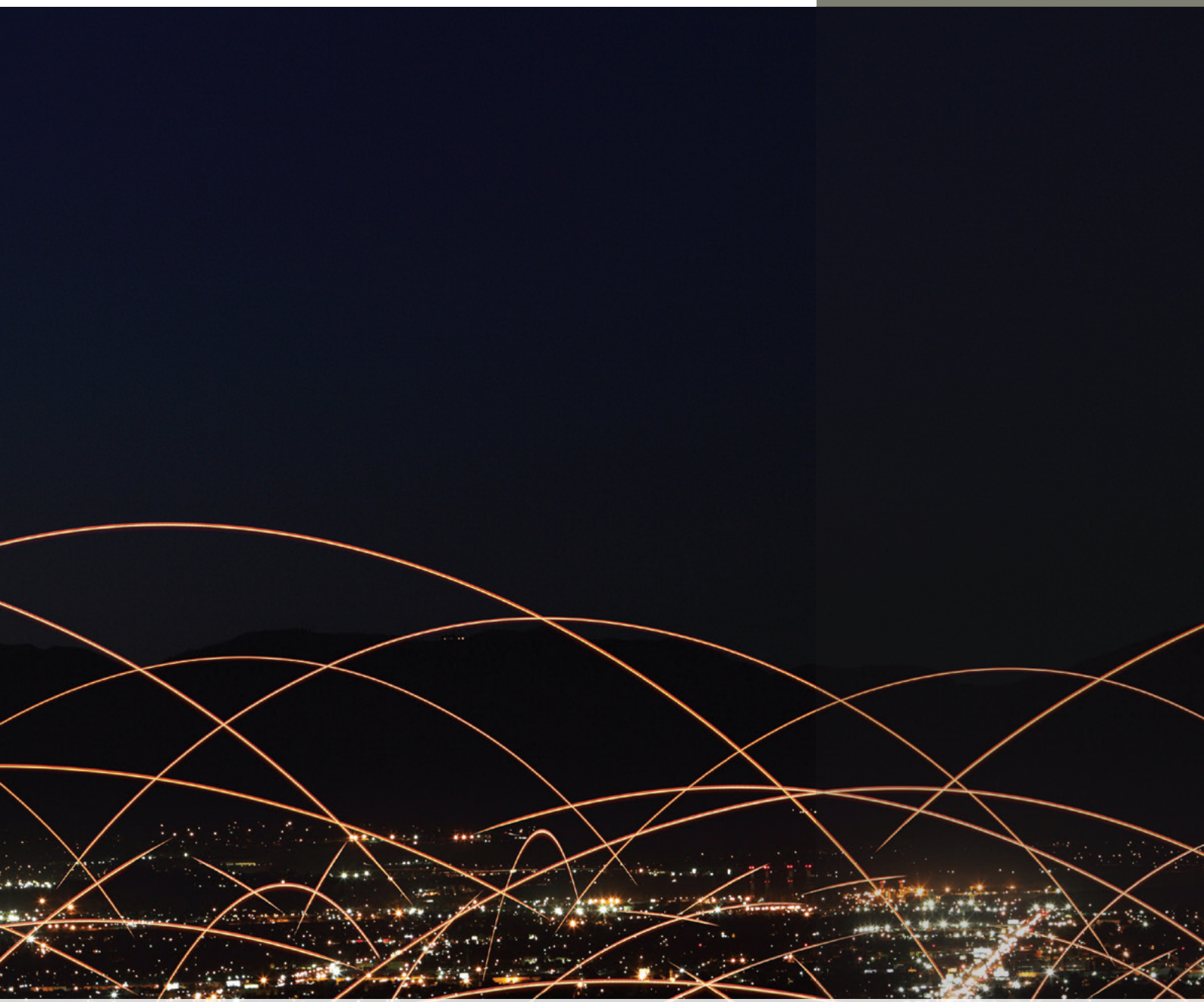
FORTINET

SOLUTIONS GUIDE



Connect & Secure

Secure, Cost-effective, Unified Access for the Distributed Enterprise.

Executive Summary

In recent years, the ever-shifting goal posts of enterprise security have been radically redefined by a revolution in mobile access. The increasing ubiquity of smart mobile devices, together with advances in 802.11xx wireless LAN technology, has led to a proliferation of wireless usage throughout the enterprise, often creating overlay networks where the access security policy differs to that of the existing wired infrastructure. This has not only complicated the task of management, but opened up new vulnerabilities, compromising the overall security of the network.

Over the same period - most notably perhaps in the retail sector – we have seen a disturbing rise in the number of highly publicized data thefts, as cyber-criminals exploit such vulnerabilities in increasingly sophisticated ways.

As a result, traditional, centrally-deployed defenses are no longer adequate, yet replicating these defenses at hundreds or even thousands of remote locations is not only costly, but can greatly increase management complexity.

The answer is Fortinet's Connect and Secure, a tightly integrated, centrally-managed, unified access solution, in which comprehensive, multi-layered security extends automatically with each new network connection, wired or wireless. Connect & Secure encompasses Fortinet's Secure Access Architecture, integrating comprehensive security with a unified access layer to provide enterprises with the level of wireless security required in today's demanding and changing environment.

The Big Problem

• Business demands fast, transparent access to critical applications and data, from anywhere, and from a range of devices over which administrators no longer have full control.

• There are obligations to customers, business partners and shareholders, as well as regulatory mandates, to properly secure business data and applications from unauthorized access.

• Security threats are rapidly increasing in number, risk, and sophistication.

• Capital and operating budgets are not rising in proportion to the challenge.

For large, distributed, customer-facing organizations, for example in retail, hospitality, or the restaurant sector, these challenges can be further complicated by a requirement to provide guest access to network services and to the Internet.

Such trends further erode any remaining notion of a network security perimeter to the point where every remote branch of a distributed organization must now be considered a potential entry point for malicious attack.

Although the preferred targets of such attacks remain centrally located resources such as the customer database (most often breached using well-known techniques such as SQL injection), analysis of recent high-profile intrusions has often traced the initial entry point to vulnerabilities on remote or wireless client devices. In the case of retail, such devices may even include network attached Point of Sale (POS) terminals, many of which run embedded versions of Microsoft Windows, and which are now being targeted directly by an expanding range of new malware variants specifically designed to steal customer credit-card details.

One response to these heightened risks has been to replicate the same central layers of security at each remote location, but this creates its own challenges. Not only can such an approach be prohibitively expensive in terms of increased hardware and software licensing, but the configuration and maintenance of these solutions often requires a level of on-site technical skills previously limited to the central headquarters.

A far better solution is to embed security into the network infrastructure itself, so as the network is extended through new wired or wireless access points, security is imposed automatically with each new connection

The 5 Key Considerations

Security

Effective protection of enterprise data and applications comprises a number of successive security measures:

• First, users must be identified, authenticated (preferably via 2-factor authentication, using both password and token), and checked for authorization to access the requested data, applications or URLs.

• Throughout the session, the user's pattern of behavior should be checked against known intrusion prevention techniques, with any anomalies flagged or logged for later analysis as required.

• Due to the existence of zero-day exploits, social engineering, and polymorphic viruses, to name but a few of the tactics employed by cyber-criminals, intrusions and malware will still occasionally slip through. When they do, it is essential to minimize the time taken to detect them, so they can be dealt with swiftly and efficiently.

• Finally, the network administrator needs to be alerted to the nature and potential impact of any detected threat, and any infected systems need to be quarantined and cleaned.

In most large organizations, the majority of these security measures will already be applied centrally, but as we've just seen, with the recent proliferation of wireless access, this is no longer enough. Unless a common unified security policy can be applied to all new points of access, wired and wireless, the risk of leaving open an unguarded backdoor remains unacceptably high.

Connectivity

Fundamental to any secure network solution is the provision of flexible wired and wireless connectivity options that can scale as new equipment and personnel are added or moved from one location to another.

Authentication aside, all network access needs to be transparent to the user. Whether querying the customer database or making an IP voice call, response times need to be as fast via WiFi as via Ethernet. With WiFi speeds now pushing 1.3 Gbps, this is not only achievable, but increasingly the most cost-effective option for new network builds, with some organizations now foregoing wired connections altogether.

And with most large organizations now embracing 'Bring Your Own Device' (BYOD) policies to a greater or lesser degree, ubiquitous high-speed wireless coverage is often a mandatory requirement.

Performance

Although high-speed wired and wireless access devices are now readily available and relatively inexpensive to deploy, the challenge comes when you start to integrate the aforementioned security measures. This is because the kind of traffic analysis required to provide such protection can be highly processor-intensive.

It is therefore critical that any unified access and security solution not only meets current requirements in terms of bandwidth and latency, but has the architecture to scale to future demands as well.

Cost

Security will always represent a compromise between risk and cost. Spend nothing at all on security and the risk of serious breach approaches certainty. Impose too many hurdles between users and the data and applications they need to do their jobs, and the cost, both in financial and productivity terms, becomes prohibitive.

But calculating the true cost of a security solution is not straightforward. Not only are there capital and operating costs to consider, but also the potential cost to the business resulting from each breach. In today's landscape of advanced persistent threats, some level of intrusion is inevitable, but for any given attack, its subsequent impact on the business can vary enormously depending on how it is managed. The longer it takes to detect, quarantine and eradicate the problem, the greater the impact to productivity, and the higher the subsequent clean-up costs.

Manageability

In addition to the basic network management requirements of central configuration and monitoring, security adds several more layers of complexity. For example the system may need to integrate with third-party authentication servers based on Radius or ActiveX. Additionally, in the event of a security breach, the network administrator not only needs to be alerted, but presented with a range of remedial actions to resolve the problem. Furthermore, to remain effective, the system needs to be able to learn from past breaches and ideally, the input for this learning should come not only from your network, but from thousands of others just like it.

The Solution

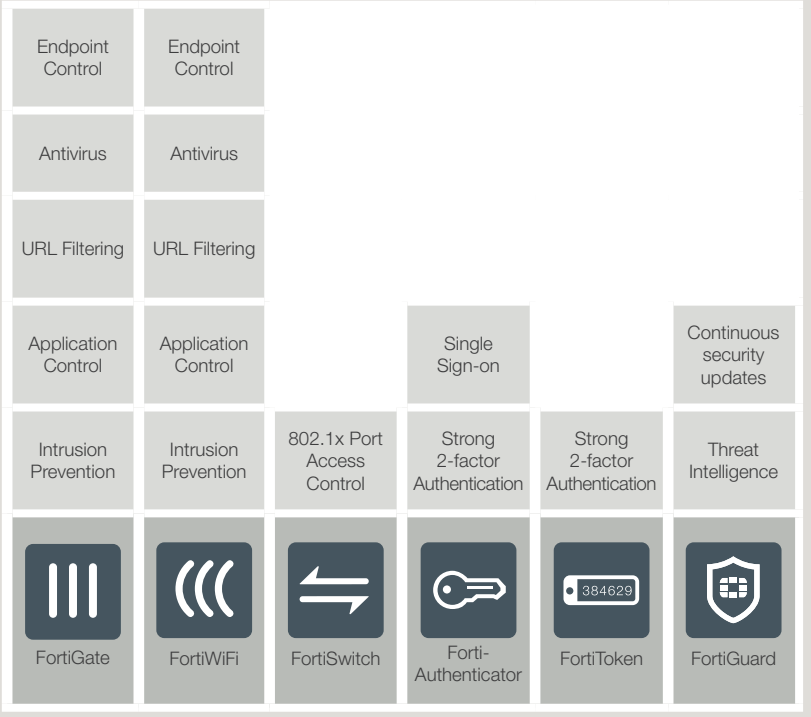
Connect and Secure is a suite of products which, acting in concert, meets each of the above challenges to provide the needed level of protection and secure unified access that automatically extends with each new network connection.

Key Benefits

Security

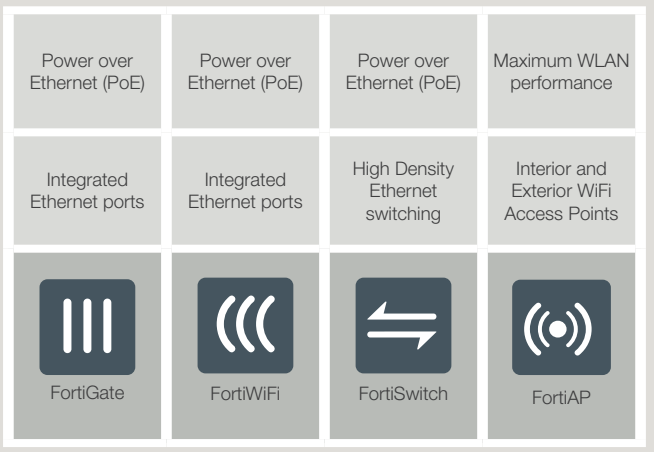
Embedded into every network infrastructure component, and tied together via FortiGate's centralized management portfolio, a comprehensive range of security measures are applied with each new connection, wired or wireless.

Furthermore, through the 24/7, automatic, threat response services of FortiGuard, Connect and Secure becomes part of a much larger, self-learning enterprise safety-net spanning thousands of Fortinet customers around the globe and thereby greatly reducing the time taken to respond to new threats.



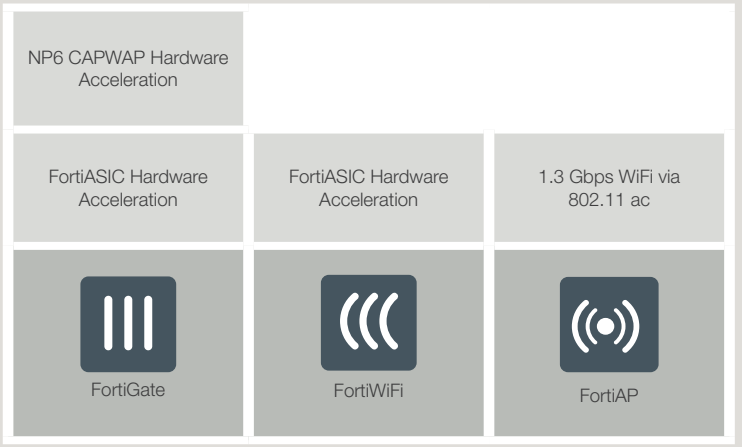
Connectivity

Connect and Secure offers a wide range of cost-effective wired and wireless connectivity options to suit all possible requirements.



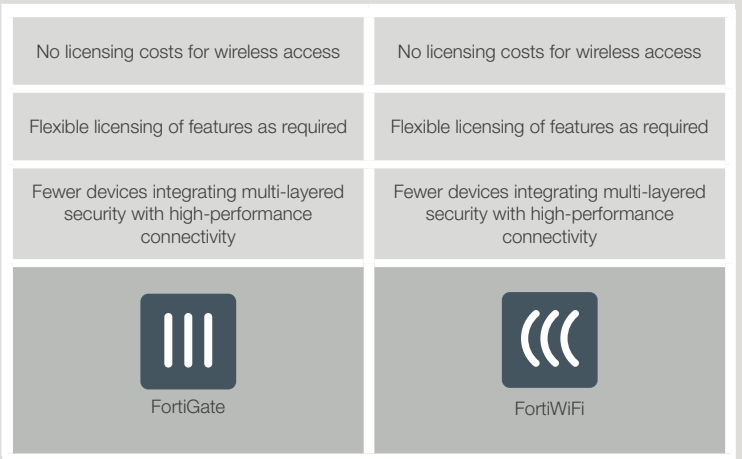
Performance

To ensure optimal throughput, even when the full range of security measures are enabled, the solution makes use of dedicated Application-Specific Integrated Circuits (ASICs) to provide hardware acceleration of key network processing functions.



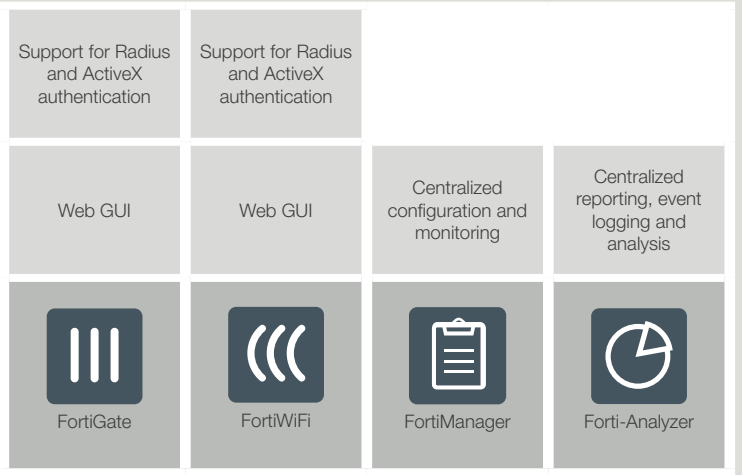
Cost

Due to the tight integration of connectivity and security, Connect and Secure requires fewer devices than competitive solutions, with no additional licensing fees for wireless access, and the flexibility to license only the specific functionality required at each location.



Manageability

Although able to extend the full range of security features with each new network connection, wired or wireless, Connect and Secure is designed to be fully managed from a central location, greatly reducing the chance of having to send trained personnel to remote sites.



Summary

Connect and Secure is a scalable and cost effective secure unified access solution, providing both connectivity and security for the distributed enterprise. With Connect & Secure, enterprises can confidently deploy a decentralized security infrastructure and provide full wired and wireless connectivity throughout the network. Secure Ethernet and WiFi connectivity are provided via the FortiGate and FortiWiFi network security appliances. Both FortiGate and FortiWiFi support integrated Ethernet ports but if and when additional connections are required, Ethernet connectivity can be extended with high-speed switches with FortiSwitch. Secure wireless connectivity is integrated in the FortiWiFi for smaller locations while larger sites are supported through FortiAP secure access points. In both cases, due to the integrated controllers in the FortiGate, both the FortiSwitch and FortiAP effectively become extensions of the FortiGate, without any gaps or vulnerabilities to be exploited.

The embedded security of these highly flexible and scalable infrastructure components comes from a combination of their operating system, FortiOS, the FortiAuthenticator and FortiToken authentication solutions, and the automated, 24/7, self-learning, continuous threat response resources of FortiGuard.

Management of the infrastructure, which is all consolidated through the FortiGate, is accomplished via FortiManager and FortiAnalyzer, combining centralized configuration with reporting, event logging and analysis, to create a comprehensive, real-time network monitoring and control centre.

Together, these products all integrate seamlessly to deliver *Secure, Cost-effective, Unified Access for the Distributed Enterprise*.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480