

# MANAGED FIREWALL & NETWORK SECURITY

## SECURITY

## Protect your entire attack surface with advanced security

### CHALLENGES

Organisations under constant attack cannot afford to choose between security and maintaining a high-performance business infrastructure. From branch to campus to deep within internal segments, to physical and virtual data centers, your extended enterprise needs security that won't compromise performance.

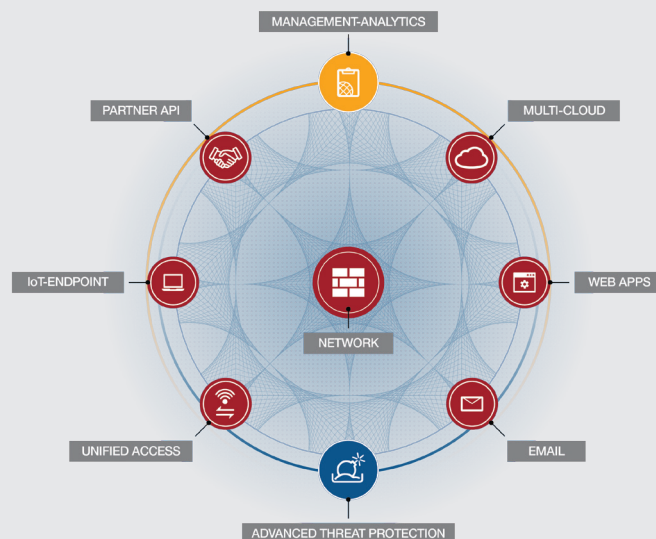
Deploying network security solutions from multiple vendors causes unnecessary complexity and introduces security gaps. **Fortinet's Network Security** solution – based on its flagship **FortiGate** product family – provides coverage and visibility for your enterprise's entire attack surface.

**Fortinet Network Security** leverages a single operating system that works across different network security use cases. It delivers industry-leading security effectiveness, unmatched performance, and reduced complexity.

## FORTINET SECURITY FABRIC COLLECTION

### How a FortiGate firewall can be set up to protect a network

The Fortinet Security Fabric links various security sensors and tools together to collect, coordinate, and respond to malicious behavior, in real time, anywhere it occurs on your network.



### AD INTEGRATION & CO-MANAGEMENT

## NEXT-GENERATION MANAGED FIREWALLS

### FortiGate: Industries best threat protection and performance with reduced complexity

- High performance, consolidated advanced security
- Deep visibility to protect against known and unknown attacks

Providing high performance, consolidated advanced security and granular visibility for broad protection across the entire digital attack surface, FortiGate enterprise firewalls reduce complexity and improve overall security posture by providing full visibility into users, devices, applications and threats on the network, with the ability to apply advanced threat protection anywhere in the network.

Their purpose-built security processors (SPUs) deliver scalable performance of advanced security services,

industry-leading VPN and SSL inspection throughput, and ultra low latency for protecting internal segments and mission critical environments. Validated FortiGuard security services protect against known and unknown threats, zero-day exploits, malware, and malicious websites using FortiGuard Labs continuous threat intelligence, dynamic analysis for detection, and automated mitigation to keep your network protected from advanced cyber attacks.

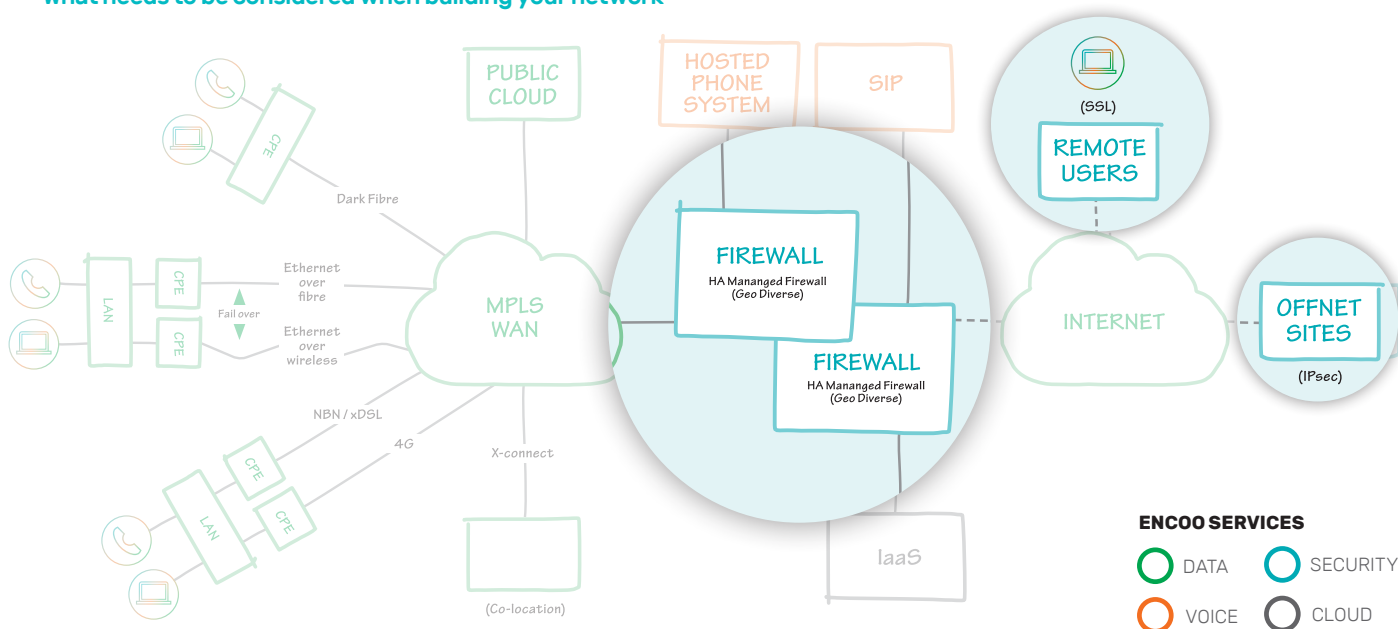
They deliver the lowest total cost of ownership along with supporting scalable, flexible deployments from the network edge to the core, data center, internal segments, and the cloud. FortiGate's are Security Fabric enabled, providing the broad visibility, automated protection and integrated threat intelligence required to protect the valuable assets and data of organisations worldwide.

## Network Security

When offering Managed Security products choosing an industry leader as your vendor of choice is only one piece of the puzzle, integrating the chosen platform into the network is equally as important. Encoo Managed Firewall is delivered using Enterprise Grade firewalls engineered by Fortinet. They are configured in a High Available (HA) cluster that reside in geographically diverse leading Data Centres. Security is absolutely paramount to any Encoo Managed WAN solution as to is availability, designing solutions in this way provides industry leading protection and multiple levels of redundancy.

### NETWORK DIAGRAM

What needs to be considered when building your network



### THE ENCOO EDGE

Encoo Managed Firewalls are delivered using a pair of Geo Diverse Fortinet Firewalls configured in HA with all UTM features enabled as standard. Want more control? Speak to Encoo today about co-management options that allow you to respond faster, have complete visibility and give you the edge over your competition.

### WHY FORTINET?

Fortinet secures the largest enterprise, service provider, and government organisations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. More than 330,000 customers trust Fortinet to protect their businesses.

**FORTINET®**

# NETWORK SECURITY – ADDITIONAL SERVICES

## SECURITY

### Enjoy greater peace of mind

Complementing the Fortinet Managed Wirewall solutions, there are a number of network security 'bolt-on' products that can be provided and implemented into a network to bolster protection against threats, creating a more robust solution.

#### FORTIMAIL NETWORK SET-UP

How Fortinet 'bolt-ons' can be used to secure a network

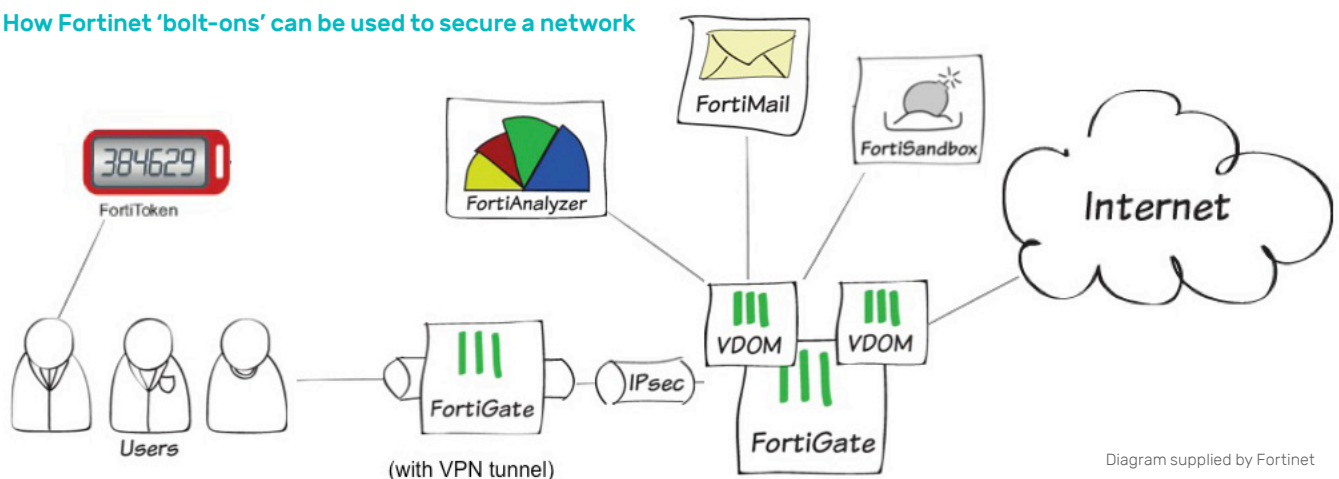


Diagram supplied by Fortinet

#### FORTIMAIL

##### EMAIL SECURITY

A secure email gateway (SEG) is designed to block ransomware, phishing, and other cyber threats seeking entry via incoming email, while ensuring that outgoing messages don't improperly leak sensitive data. These are critical capabilities given that (according to Verizon's 2017 Data Breach Investigations Report) two-thirds of malware was installed via email attachments. Email was also the most common entry point for ransomware, costing organizations an estimated \$850 million last year. SEGs also help ensure compliance with a wide range of data privacy regulations and corporate mandates to protect intellectual property.

##### FortiMail includes:

- Consistently demonstrated 99%+ antispam effectiveness to save employee time
- Top-rated anti-malware protection (including sandboxing) to stop ransomware, phishing, and other email attacks
- Robust data loss prevention (DLP) features, including predefined dictionaries, identifiers, and digital fingerprinting to simplify compliance with privacy regulations
- Identity-based encryption to securely deliver messages containing sensitive data
- Integrated email archiving to meet legal and regulatory retention requirements as well as e-discovery

## FORTISANDBOX

With the increasing volume and sophistication of cyber-attacks, it takes only one threat to slip through security for a data breach to occur. CISOs have adopted sandboxing as an essential component of their security strategies to help combat previously unknown threats. While attack surfaces are becoming more dynamic due to the rise of IoT and cloud-based services, a continuing shortage of cyber security talent is driving organisations to integrate sandboxing with greater controls and a high degree of automation.

### FortiSandbox includes:

- Critical protection against advanced and emerging threats
- Broad integration with Fortinet and third-party security solutions to help protect an organisation's dynamic attack surface
- Automated sharing of threat intelligence in real time to disrupt attacks early in the cycle without human intervention
- Flexible form factors to help support various industry requirements

## FORTITOKEN

### One-Time Password Application Software Token

Passwords alone don't keep unwanted guests out of your network. Password-only authentication has led to security breaches, malware infections, and policy violations. With two-factor authentication, a password is used along with a security token and authentication server to provide far better security. Authorized employees can access company resources safely using a variety of devices, ranging from laptops to mobile phones.

FortiToken Mobile is an application for iOS or Android that acts like a hardware token but utilizes hardware the majority of users possess, a mobile phone.

## FORTIANALYSER

### CENTRALISED NETWORK SECURITY LOGGING AND REPORTING

Lack of visibility continues to extend breach and compromise events to an average of more than 100 days. For each day an organization is exposed, it's another opportunity for attackers to get to sensitive customer and confidential information.

FortiAnalyzer provides a consolidated view across Fortinet devices throughout your organization with real-time alerts that expedite the discovery, investigation, and response to incidents even as they're happening. With action-oriented views and deep drill-down capabilities, FortiAnalyzer gives organisations critical insight into threats across the entire attack surface.

### FortiAnalyzer includes:

- Centralised logging, reporting and event correlation
- Powerful NOC/SOC dashboard
- Automated indicators of compromise (IOC)
- Real-time and historical views into network activity

**For more information on complementary products, please contact Encoo Communications today.**

### THE ENCOO EDGE

Co-management of client facing VDOM's, AD Integration and automated reporting provides channel partners with real time visibility and control over the end clients security framework. Meaningful and detailed reports allow channel partners to present to C-Level stakeholders on the threats that are being tackled on a daily basis, as well as demonstrate a return on investment, which is often difficult to do with hardware that is procured 'as a Service'.

## WHY FORTINET?

Fortinet secures the largest enterprise, service provider, and government organisations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. More than 330,000 customers trust Fortinet to protect their businesses.

**FORTINET®**