Intelligent Business Solutions Ltd

# BEST PRACTICES TO SECURE YOUR CORPORATE NETWORK WITH FORTIGATE

By Kyriakos Ioannou – Systems Engineer

## What is FortiGate?

FortiGate is a next-generation firewall that utilizes purpose-built security processors and threat intelligence security services from AI-powered FortiGuard labs to deliver top-rated protection and high-performance inspection of clear-texted and encrypted traffic.

## Recommended Security Best Practices

- **Unauthorized access layer devices**

All access layer devices such as wireless access points and network switches should be identified and validated. Unauthorized devices should be immediately disabled.

- **Secure Wireless Connections**

All Wireless networks should not permit insecure protocols such as WEP or other less secure algorithms.

- **Review unused policies**

All firewall policies should be reviewed every 3 months to verify the business purpose. Unused policies should be disabled and logged.

- **Segregation of Traffic**

Separate servers from end user devices.

- **VLAN Change Management**

VLAN changes should be updated to all firewalls in the Fabric.

- **Third Party Router & NAT Devices**

Third party router or NAT devices should be detected in the network.

- **Device Discovery**

Ensure that all systems are detected and logged on internal networks, including DMZ.

- **Interface Classification**

All network interfaces should be assigned a defined and configured based on the security risk profile of the segments and systems being protected.

- **Detect Botnet Connections**.

Ensure all networks including wired and wireless access points are configured to detect Botnet activity, including any similar suspicious traffic entering and leaving the network.

- **Explicit Interface Policies**

Security policies should permit only authorized least privilege and least required traffic to/from authorized systems.

- **Secure Remote Access**

All remote access included site-to-site and personal VPN should require at a minimum 2-Factor authentication.

- **Double-NAT**

Identify if the Security Fabric is performing Network Address Translation multiple times to any traffic pathway.

Kyriakos Ioannou is working as a systems consultant with IBSCY LTD for the last 4 years. He is a member of the maintenance and support team responsible for the day-to-day support of our clients in Cyprus and internationally. He is also running small to medium size projects of office 365, Windows Azure and infrastructure. He holds several certifications of Microsoft, HPE and other vendors.