SERVICE DESCRIPTION

Managed Firewall

Executive Summary

Thrive Managed Firewall Service Definition

Thrive Managed Firewall Service provides fully managed edge security utilising the Fortinet FortiGate Unified Threat Management platform. The service includes the physical or virtual FortiGate firewall with full monitoring and management of the firewall configuration, policies and rules.

Services Scope

The service shall include:

- Fortinet FortiGate firewall device(s) as indicated in the Thrive Service Order including subscriptions for optional services below where applicable
- Stateful packet filtering
- Network Address and Port Address Translation
- 10 configuration changes per month per device
- 1 DMZ
- 3 VLAN's
- Regularly scheduled review of firewall firmware and base configuration to confirm compliance with Thrive standards
- OPTIONAL add-on services
    - Intrusion Prevention Service
    - Web Filtering
    - Gateway Anti-Virus/Anti-Spyware
    - VPN Service
        - FortiClient VPN Connectivity Only
        - Split-tunnel VPN Routing Policy with networks local to FortiGate Firewall to be included by default within VPN policy
        - VPN connectivity to multiple sites supported if there is established connectivity between those sites and the site hosting the Thrive Managed FortiGate
        - SSLVPN Portal configured with default self-signed SSL certificate unless certificate provided by customer
        - FortiGate will be configured to assign IP addresses to VPN clients
        - MFA (multi-factor authentication) requires Azure Active Directory integration with appropriate Azure licensing; other identity providers may require a separate change order at additional cost

Thrive Scope of Work and Deliverables

- Thrive shall configure the Managed Firewall in accordance with Client's defined requirements. Upon activation of the Managed Firewall Service Client is responsible for confirming that the configured firewall is in accordance with Client's preferences and all appropriate and potentially impacted services are functioning as expected
- Upon completion of installation and upon Client request, Thrive will administer all changes and modifications to the firewall rule sets and configurations. Basic configuration changes include such actions as:
  - Firewall rule set modification
  - Device firmware upgrades, configuration backup and recovery as needed
  - Problem, Incident, and Change Management
- Thrive shall perform a regularly scheduled review to confirm firewall is in accordance with Thrive's documented firmware and base configuration standards
- Thrive shall be responsible for the ongoing hardware and firmware maintenance of the firewall service.

- OPTIONAL Firewall Web Filtering Service Add-on
  - If included in the Thrive Service Order, Thrive shall provide client documented Thrive standards for Web Filtering configuration. An additional one-time cost may be incurred by client if customisations to Web Filtering configurations are required.
- OPTIONAL Firewall Protection Service (Antivirus/Anti-Spyware) Add-on
  - If included in the Thrive Service Order, Thrive shall configure firewall antivirus/anti-spyware policies according to Thrive standards and cybersecurity best practices. An additional one-time cost may be incurred by client if customisations to Antivirus/Anti-Spyware configurations are required.
- OPTIONAL Firewall Based Intrusion Prevention System Add-on
  - If included in the Thrive Service Order, Thrive shall configure firewall Intrusion Prevention System policies according to Thrive standards and cybersecurity best practices. An additional one-time cost may be incurred by client if customisations to Intrusion Prevention System configurations are required.
- OPTIONAL VPN Service Add-on
  - Thrive shall configure the FortiGate SSLVPN in accordance with specifications defined within the Service Definition. Customisation may require a separate change order at additional cost
  - Thrive is responsible for troubleshooting and resolving issues specifically related to the FortiGate SSLVPN configuration or its availability

Client Responsibilities

- Client shall provide Thrive with sufficient information and documentation necessary to properly setup, configure, install & manage the Managed Firewall Service. If Client is unable to provide information, Client may elect to have a Thrive engineer review any existing firewall configurations to gather required information for an additional fee.
- Client shall provide the Thrive Deployment Engineer with all LAN/WAN IP Schemes.
- Client shall provide Client escalation contacts to Thrive for service event notification.

- Client shall provide the appropriate space, power, and cooling for the firewall as specified by the equipment manufacturer.
- Client shall allow Thrive to install firmware upgrades, critical updates and patches based on the Thrive provided maintenance window, or provide Thrive with scheduled and emergency maintenance windows as needed to install firmware upgrades, critical updates and patches.
- OPTIONAL VPN Service Add-on
    - Client shall be responsible for distribution and installation of the FortiClient VPN Only client to user endpoints unless endpoints managed by Thrive
    - Client shall be responsible for configuring and managing 3rd party identity or authentication providers unless provider is managed by Thrive
    - Client shall be responsible for troubleshooting and/or resolving issues related to 3rd party identity or authentication providers not managed by Thrive
    - Client shall be responsible for troubleshooting and resolving network connectivity issues to destinations not supported by Thrive

Service Limitations

- Client acknowledges and agrees that the Managed Firewall Service constitutes only one component of an overall security program and is not a complete and comprehensive security solution.
- Firewall hardware and software platforms have vendor specified bandwidth throughput and connection limitations which are impacted by the security features selected for activation by the Client. Thrive will consult with the Client to select the appropriate firewall platform based on information provided during the initial consultation to review security requirements. Security services that are activated at the request of the Client after the initial consultation or firewall configuration that negatively impact the performance of the hardware and software are the responsibility of the Client. Thrive will work with the Client to select another firewall platform that may result in additional monthly fees.
- Service does not include the vendor management of the Internet Service Provider (ISP) or Wide Area Network (WAN) carrier.

Equipment Return

Upon termination or expiration of the Managed Firewall Service, Client shall return all hardware and software components of the firewall system provided by Thrive to Thrive at Client's expense. If Client fails to return all components of the firewall system to Thrive within 10 days after termination or expiration, Client will continue to be liable for and obligated to pay monthly recurring charges for the Managed Firewall Service.

Service Exclusions

Any service not explicitly included in the Thrive Sales Order or Managed Firewall Service Definition above is considered optional and may be provided under separate agreement for an additional fee.