Service descriptions: Firewall management, monitoring and threat hunting services

Version: 2.3

Date: 2021-01-23

Confidentiality: PUBLIC

FORESIGHT™ CYBER

CONTENTS

1 SERVICE OVERVIEW

Network firewalls still play a key role in any well-balanced cyber security strategy. New technologies embedded into network firewalls have shown to successfully fight today's threats that attack companies' systems and users. As the complexity of the firewall increases, the underlying management increases correspondingly bringing additional challenges for internal IT teams.

Foresight Cyber has recognised that this shift in technological and procedural complication increases risk and offer a superior firewall management service that helps organisations overcome these burdens.

Our services are structured to fit each client's needs as follows:

The Silver level: Firewall Platform Management ensures that your firewall(s) are continually operational, maintained with appropriate system updates, and all available features provided by your firewalls are managed confidently.

The standard Service Level Agreement (SLA) delivers timely changes and standard availability incident resolution. While firewalls are monitored by our fully automated Foresight Cyber Platform, the resolution of any issues and implementation of required changes occurs during London business hours.

The Gold level: in addition to the Silver level adds a risk- related service by reviewing requested changes and annual recertification of the firewall rules for applicability. The SLAs of the service provide faster response times.

The Gold level offers an optional 24x7 management element.

The Platinum level: in addition to the Gold level adds threat hunting by collecting security logs from the firewalls, enriching with open-source threat intelligence data (OSINT): using a specially designed rulebook to find actual threats and incidents. The more data points we get from the customer, such as DHCP, AD and server logs, the superior the hunting service becomes.

The Platinum level offers an optional 24x7 management element.

Service levels at glance

	Silver	Gold	Platinum
Real-time automated monitoring	Included		
Software updates *	Included		
Firewall rules management *	Included		
Firewall rules management with analysis of firewall changes for compliance and risk *	Included		
Annual firewall re-certification *	N/A	Included	
IDS package management	Included		
Proxy anti-malware package management	Included		
Site to Site VPN setups & management	2 per firewall pair	8 per firewall pair	20 per firewall pair
High-availability setup & management	Included		
User SSL VPN setup & management	2 profiles	4 profiles	8 profiles
SLA to implement changes (business hours)	16 hours	8 hours	2 hours
SLA to begin fixing incidents (business hours)	4 hours	2 hours	1 hour
Read-only access to configuration and logs	Included		
Reporting portal	Included		
Included changes per Firewall per year	10	20	30

* required for CE+ (https://www.ncsc.gov.uk/cyberessentials/overview)

Unless specified in a contract, the 'business hours' are defined as 8am to 5pm local London time, Monday to Friday.

2 FIREWALL SERVICES DESCRIPTION

With our upgraded firewall management service, we support the installation, configuration, on-going management and monitoring for the following technology vendors:

- PFSense on Netgate HW, or our certified HW, or as a virtual appliance,
- Watchguard HW appliance

2.1 Silver Service components

For the above technologies, we provide, subject to SLAs, the following services.

2.1.1 Monitoring availability

We add all firewalls to our monitoring system provided in Foresight Cyber Platform©. This will alert our team to any potential availability issues and maintain appropriate firewall performance reports. We will also advise clients when a HW firewall or virtual appliance is at 80% of its average capacity.

2.1.2 Software updates

We will ensure that the firewall software is always at the latest stable version, unless the functionality required is no longer supported, or where a risk assessment has shown that a temporary delay is required, e.g. because a critical business operation occurs simultaneously. Security updates to the firewall operating system and applications are installed as per our vulnerability management policy unless a client requires a more stringent policy to be applied.

2.1.3 Implementation of firewall changes

All changes to firewall configurations, requested and approved by a client, will be implemented according to strict requirements of the agreed change management process. This will include taking a backup of the configuration before the change, and agreed date and time for change, together with a follow up communication with the client after the change. In our own process, a change is not labelled as 'Completed' until the changes are thoroughly tested. As part of our standard security management, a log of all firewall changes is meticulously maintained.

The following change types are included in the service. Adding, modifying, and removing ruleset objects (typically a user, user group, host, host group, application

- Adding, modifying, and removing firewall rules

- Changing parameters of firewall licensed security modules and configuration of the firewall itself

Other changes are charged on time basis using our standard hourly/daily rates. The following are not exhaustive examples of non-standard changes, these are typically those that would typically require a design document update, a detailed review by our firewall consultants and a discussion with a customer:

- Changes to physical, virtual interfaces and VLANs
- Changes to firewall routing
- Setting up a new private virtual network (VPN)

2.1.4 Reviewing firewall rules requests

We will undertake a review of change requests for security risks and compliance issues and advise the client appropriately. We use our best practice, NIST 800-41 as well as industry best practices relevant to the client profile and their environments.

2.1.5 Management of advanced threat monitoring and protection features

As standard, the Intrusion Detection System (IDS) component is implemented on all firewalls, unless instructed by the client not to do so. On request, and after careful consideration, we can also enable rules in blocking mode.

All firewalls are configured with daily updates of malicious IP addresses and with client agreed rules to block traffic from and to these IP addresses.

2.1.6 Management of Remote access

We configure and manage remote access configuration, typically by SSL or IPSec VPNs. We support internal firewall authentication, certificates or external RADIUS authentication and authorisation.

2.1.7 Management of site-to-site VPNs

On request, we will setup and manage site-to-site VPN connectivity between client sites, or the client site and a 3rd party partner. For the latter, we will require assistance from and work with the 3rd party firewall or network team.

2.1.8 Management of high-availability clusters

We manage high-availability clusters to ensure continuation of service in case of HW or SW failure.

2.1.9 Management of Web proxy function

On request, we will configure an explicit proxy function on firewalls. The proxy server will be configured to prevent or report traffic to malicious domains, and this may also be used to monitor access to sites in breach of company's code of conduct if the client so wishes.

2.1.10 Security and compliance reporting

We provide monthly reporting to the client that includes availability statistics, changes performed, any service issues encountered, and threats as detected by the firewall software.

2.2 Gold Service Components

The gold service adds annual rules recertifications and enhanced SLAs.

2.2.1 Annual re-certification of all firewall rules

On an annual basis, we will issue a request to the client to re-certify all firewall rules. This process forms part of the primary certification standards and helps maintain effective and efficient control of both ingress and egress to the network.

2.3 Platinum Service Components

2.3.1 Security event monitoring and threat hunting

As part of our service, we setup a log collection service and ingest firewall logs. Depending on the platform and firewall modules enabled, we monitor for security, availability and change events. We use these events for reporting and to trigger security responses as appropriate.

Our automated platform is supported by a team of experienced security operations analysts who review flagged events and make decisions if these require investigation and reporting to a client.

3 OPTIONAL SERVICES

The following are optional services that can be purchased.

3.1 24 x 7 Management

Available for customer opting for the Gold and Platinum firewall service.

4 ADDITIONAL INFORMATION

4.1 Client access to firewalls

On request, we will supply read-only access to the firewall configuration, all changes and approvals relating to managed firewalls.

We will also copy firewall logs – audit, traffic, and application specific – to the client's log management tool. We do not permit sharing firewalls between two or more clients, thereby negating any possibility of accidentally disclosing other clients' data.

4.2 Contacting our support team

Our service is designed to be semi-automated: therefore, it is extremely important that communications between the Foresight Cyber support team and the client team is always maintained as closely as possible.

Our support team is accessible via email and Microsoft Teams – individual engineers have named accounts, and these are shared with customers at the start of the service.

4.3 Service requirements

To deliver the best service possible, we require the following:

- Setup of a site-to-site VPN to our Foresight Cyber Operations Centre used for management, automatic monitoring and backup operations
- For increased monitoring levels, we require the installation of Foresight Cyber Out of Band (OoB) appliance and providing Internet connectivity, or setup an independent Internet connection – subject to specific agreement. This OoB appliance is then connected to the firewall using either Console or Ethernet cable.

The connection is only used when the site-to-site VPN is not working correctly, as per agreed processes/protocols

- PKI certificates for your users' remote access, unless you require us to create certificates for those users
- A list of whitelisted IP addresses and domains – typically your business partners and key business web sites
- Acceptable use policy for optional proxy service including permitted / prohibited website access monitoring and alerting for attempts to exploit the vulnerability of Foresight Cyber Security's systems.

FORESIGHT CYBER LTD

Registered & Business address UK
71-75 Shelton Street,
Covent Garden
London
WC2H 9JQ
United Kingdom

Business address CZ:
Fryštátská 64/9
733 01 Karvina
Czech Republic

Contacts:
UK Office: +44 20 8159 8942
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber.com

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017