Managed Web Content Filtering

Service Overview

Web Content Filtering (the "Service") is provided on a Fortinet next generation firewall appliance with 24x7x365 proactive administration and monitoring of your Fortinet firewall appliance. Certified security experts will perform all activities necessary to keep the Web Content Filtering enabled Fortinet appliances operating at peak performance.

Service Objectives: Web Content Filtering service provides the customer with the following:

- 24x7 Monitoring of your web site traffic, blocking access to malicious, hacked or inappropriate websites
- 24x7 Service support with online portal access to web content whitelist/blacklist capabilities, ticketing and alerting
- Event/Incident triage with security service support. Triage will work towards identification and remediation.
- We will provide alerting based on log events matching malicious behavior.

Service Deliverables: SILVERSKY's Web Content Filtering service will deliver to the customer the following:

- Fortinet Web Content Filtering enabled on Fortigate firewall device
- Web Content Filtering Whitelist/Blacklist, IP block controls
- Monitoring and Alerting for malicious website events
- Portal access to web content filter settings and configuration with service ticketing

Service Description

A proprietary threat intelligence platform provides the foundation for delivery of our Web Content Filtering service. Web Content Filtering will block access to malicious, hacked, or inappropriate websites. As web filtering is the first line of defense against web-based attacks, Web Content and Filtering focuses on malicious or hacked websites, a primary vector for initiating attacks, trigger downloads of malware, spyware, or risky content.

The Web Content Filtering service is available through FortiGate next generation firewalls and includes:

- Block or Allow access to Websites based on category or rating
- Block access to known malicious or blacklisted websites
- Implement groups to control user level access to sites

Block or Allow access to Websites based on category or rating

Protect your organization by blocking access to malicious, hacked, or inappropriate websites with FortiGuard Web Filtering. Web filtering is the first line of defense against web-based attacks.

Block access to known malicious or blacklisted websites

Malicious or hacked websites, a primary vector for initiating attacks, trigger downloads of malware, spyware, or risky content.

FortiGuard Web Filtering is the only web filtering service in the industry that is VBWeb certified for security effectiveness by Virus Bulletin.

Implement groups to control user level access to sites

The web filtering service is available through FortiGate next generation firewall solutions letting you easily see and control what websites your users are visiting through user level access control of groups.

Other Services

Any other services are out-of-scope. Upon request, SilverSky may provide out-of-scope technical support on a time and materials basis pursuant to a separate service description or statement of work ("SOW"). Examples of such out-of-scope support include but are not limited to:

- On-site installation and provisioning of device
- Integration of complementary products that are not managed by SilverSky (e.g., antivirus software; web reporting software)
- Custom analysis and/or custom reports
- Forensics
- Any change requests not specified above
- Rule set design, validation, and troubleshooting
- Policy Auditing, Policy/Rule Utilization, and Security Best Practice Consulting

CUSTOMER REQUIREMENTS

Customer agrees to perform the following obligations and acknowledges and agrees that SILVERSKY System's ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

Hardware/Software Procurement

The Customer is responsible for purchasing the firewall hardware and service necessary for SilverSky to deliver the Service. Additionally, the Customer is responsible for ensuring that their hardware/software stays within Fortinet's supported versions. SILVERSKY System's SLAs will not apply to platforms that are end of life, end of support, or are otherwise not receiving updates by Fortinet.

Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance for the Customer-owned firewall and connectivity to prevent network performance degradation and

maintain communications between the customer's contracted firewall devices and SILVERSKY System's security operations centers (Secure Operations Centers" or "SOC(s)").

RMA Responsibilities

The Customer is responsible for initiating and fulfilling the return materials authorization ("RMA") process directly with SilverSky in the event that the hardware/software being managed by SilverSky is determined to be in a failed or faulty state and requires replacement.

Connectivity

Customer will provide access to Customer-premises and relevant appliance(s) necessary for SilverSky to manage and monitor the contracted firewall devices. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the SILVERSKY SMC customer portal. Service activation which may require device downtime will depend on customer deliverables such as on-site assistance with initial configuration of the appliance to get connectivity between Fortinet appliance and SilverSky data centers. SLAs will not apply to devices that are experiencing Customer-caused connectivity issues.