VPN Service

Service Overview

VPN Service (the "Service") provides IPSEC and SSL VPN Connections between locations. These connections are necessary for secure communications that support SSL authentication. Using RADIUS, LDAP and Two Factor authentication, SILVERSKY System's VPN service securely manages and monitors your connections for your business needs.

Service Objectives: VPN service provides the customer with the following:

- 24x7 Monitoring and Management of VPN Tunnels and Tokens
- 24x7 Service support with online ticketing and alerting through the customer portal
- Remote User Access to customer network and systems
- Maintenance of password changes per user request
- Event/Incident triage with security service support. Triage will work towards identification and remediation
- Protection against outside attacks and intruders

Service Deliverables: VPN service will deliver to the customer the following:

- Customer requested hard or soft VPN user tokens
- Network design and setup of VPN Tunnels between locations
- Maintenance and management of VPN users and tunnels
- Monitoring of VPN traffic and users
- 24x7 SILVERSKY security support coverage

Service Description

VPN service is an important part of your network, which allows secure connections between end users, end points and locations. We will monitor and manage VPN connections to ensure uptime and security from a number of attack types. VPN service when combined with our Managed Security Service protects your network from the latest application vulnerabilities, bots, and suspicious URLs.

- Build, Manage and monitor IPSEC and SSL VPN Connections
- Support SSL Authentication through RADIUS, LDAP and Two Factor Tokens

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.