PRESIDIO®

Palo Optimization Services

STATEMENT OF WORK

FCG - Fulton County Government

SOW Date: February 17, 2026

Opportunity #: 1001726059254.1

Valid for: 60 Days

www.presidio.com

CONTACT INFORMATION

Client Name: FCG - Fulton County Government	**Account Manager:** Catherine Bowen
Contact Name: Terrence Slaton	**Account Manager Email:** cbowen@presidio.com
Contact Phone: 404-612-0010	**Solution Architect:**
Contact Email: terrence.slaton@fultoncountyga.gov	**Sales Overlay Manager:**
Contact Address: 141 Pryor St Atlanta, GA 30303-3444	**Sales Overlay Manager Email:**

1. EXECUTIVE OVERVIEW

1.1. Project Introduction

Presidio is pleased to propose the following solution to FCG - Fulton County Government (“Client”). This Statement of Work (“SOW”) defines the tasks to be performed and the responsibilities of Presidio and Client.

The Professional Services as stated within this SOW are subject to and shall be governed by Presidio’s Terms of Service Agreement (https://presidio.com/presidio-terms-of-service-agreement) which are incorporated into and made a part of this SOW by this reference; unless a valid Master Services Agreement (“MSA”) between the parties, if any, for professional services has been executed and is in force at the time any SOW is executed; in which case the terms of the Master Services Agreement shall govern to the extent that they are inconsistent with this SOW.

Presidio will be providing the services described herein through its subcontractor Palo Alto Networks ("Supplier"). Any reference to “Palo Alto Networks” or “Supplier” in this SOW will also be a reference to Presidio.

1.2. Project Summary

Supplier will provide Services on the Client’s existing network security infrastructure (“Legacy Network”) to Palo Alto Networks hardware and software offerings (collectively “Products”) and advanced features described in the Deliverables section of this SOW (the “Target Network”).

The Services will be delivered in a phased approach based on Client requirements and the Palo Alto Networks Products and functions as described below. Palo Alto Networks will provide the Services as described in the Deliverables section of this SOW.

2. PROJECT INFORMATION AND SCOPE OF WORK

2.1. Palo Optimization Services

The Target Network is a Palo Alto Networks platform running a mutually agreed-upon generally available (GA) version of PAN-OS and consisting of the elements in the following tables.

Target Network Elements	
Qty	**Target Platform**
8	PA-3220
1	PA-5220
4	PA-5250
1	Strata Cloud Manager

Target Network Cutover Information	
Cutover Events	
Remote cutover events	12
Additional Target Network Information	
Target Component	**Quantity/Description**
GlobalProtect	
Number of Deployments	1
Number of GlobalProtect Portals	1
Number of GlobalProtect Gateways	Up to 5
Number of GlobalProtect Client App Profiles	Up to 5
Number of HIP Profiles	Up to 5
SSL Decryption	
Outbound Decryption	
Number of SSL Decryption Profiles	Up to 3
Number of SSL Decryption Rules	Up to 15
Number of NGFWs (or NGFW HA Pairs) to perform Decryption	Up to 3
Inbound Decryption	
Number of SSL Decryption Profiles	Up to 3
Number of SSL Decryption Rules	Up to 10
Number of NGFWs (or NGFW HA Pairs) to perform Decryption	Up to 3
Cloud Identity Engine	
Number of Directories	Up to 7
Number of Cloud Authentication Services for supported Identity Providers	Up to 3
Number of Cloud Authentication Profiles	Up to 5
Number of Authentication Profiles	Up to 5
Number of Captive Portals	Up to 5

Target Network Cutover Information	
Number of GlobalProtect configurations/updates	1
Number of CIE Group-Based Security Policies	Up to 10
Strata Cloud Manager	
Number of NGFWs to onboard to AIOps	Up to 13
Number of HA pairs to onboard to SCM	Up to 2
Total Zone Count	Up to 25

2.2. Project Scope

The Services are limited to the Deliverables described in this SOW, as applied to the elements listed in the information section. Any design, configuration, or migration of elements in the Legacy or Target Network other than those listed will require a separate SOW.

The Project Scope shown below represents the in-scope project deliverables, with dependencies, and agreed-upon on-site/remote support.

#	Project Deliverables	On-site/Remote/Both	On-site Visits	On-site Days
1	SecOps Integration	Both	1	4
2	GlobalProtect	Remote	0	0
3	Strata Cloud Manager	Remote	0	0
4	Cloud Identity Engine	Remote	0	0
5	App ID	Remote	0	0
6	SSL Decryption - Inbound	Remote	0	0
7	SSL Decryption - Outbound	Remote	0	0
8	Threat Prevention	Remote	0	0

2.3. Deliverables

Phase Name	Activities to Complete
Kickoff	Complete Project Kickoff Meeting Create Initial Project Plan
SecOps Integration	SecOps Remote Integration SecOps Solution Documentation Kickoff/Planning and Qualification Project Management Onsite Travel Knowledge Transfer
GlobalProtect	Technical Requirements Review Base Config Configure Portal(s)/Gateway(s) Configure Agent Profile(s) Configure HIP Profile(s) Cutover Documentation - As-built Knowledge Transfer Project Management
Strata Cloud Manager, Cloud Identity Engine, and App ID	Strata Cloud Manager - Project Management Strata Cloud Manager - Internal Kickoff Strata Cloud Manager - Client Kickoff Strata Cloud Manager - Docs/Deliverables Strata Cloud Manager - Folder Structure Creation Strata Cloud Manager - Network Variables Approx Total Strata Cloud Manager - Network HA Config Strata Cloud Manager - Network Device Config Strata Cloud Manager - Network Zone: Interface Strata Cloud Manager - Mapping Strata Cloud Manager - Policy Creation Strata Cloud Manager - Close-out Cloud Identity Engine - Project Management Cloud Identity Engine - Review Cloud Identity Engine - Deploy

Phase Name	Activities to Complete
	Cloud Identity Engine - Configuration Cloud Identity Engine - Knowledge transfer and Documentation App ID - Project Management App ID - Project Kickoff App ID - Planning and Discovery App ID - Configuration and Review App ID - Deployment App ID - Handover
SSL Decryption (Inbound and Outbound) and Threat Prevention	Decryption - Discovery Decryption - Configure Decryption Profiles Decryption - Configure Policies Decryption - Update Migration/Validation Plans Decryption - Cutover Decryption - Documentation - Migration/Deployment Decryption - Documentation - As-built Decryption - Project Management Decryption - Knowledge Transfer Threat Prevention - Configuration and Review Threat Prevention - Planning & Discovery Threat Prevention - Project Management Threat Prevention - Project Kickoff Threat Prevention - Deployment Threat Prevention - Handover
Close Out	Complete Final Knowledge Transfer Session Review Final As-Built Document

2.4. SecOps Integration Service for NGFW

All Services provided by Palo Alto Networks are for the analysis of one (1) Palo Alto Networks NGFW Policy, for one (1) Security Operations (SecOps) Team. A “Security Operations Team” or “SecOps Team” is defined as an information security group responsible for monitoring and analyzing an organization's security posture on an ongoing basis.

The Services will be performed both on-site and remotely. Travel and Expenses (“T&E”) for one (1) on-site visit for one (1) consultant for a maximum of up to four (4) days are included in the price of the Services.

Service Parameters

Parameter	In Scope	Description
Number of NGFW Policy or Strata Cloud Manager Policy analysis	1	One (1) Palo Alto Networks NGFW Policy analysis or one (1) Palo Alto Networks Strata Cloud Manager Policy analysis for one (1) SecOps Team

2.4.1. Planning and Qualification Document

Palo Alto Networks will, with the Client's assistance, generate a planning document containing the findings and action plan resulting from a management call and project introduction. The management call will be used to discuss the in-depth action items required by the client to achieve the defined milestones within the project.

- Review Client Environment, including:
  - Strata Cloud Manager
    - Folders
    - Snippets
  - Palo Alto Networks Firewall
    - Security Policy
    - Decryption Policy
    - Policy-Based Forwarding
    - Security Profiles
    - Decryption Profiles
    - Zone Protection
  - Strata Cloud Manager Log Collector
- Review Client Environment Team Structure, including:
  - Firewall Change Approval Team
  - Network Operations Team
  - Security Operations Team
- Client-Provided Tech Support File for the project-scoped device(s)

2.4.2. SecOps Optimization

Palo Alto Networks will enhance the SecOps capabilities through the configuration of PAN-OS to enable features that will assist the SecOps in operational activities. All tasks for the SecOps Optimization task will be completed via remote access to the Client's production environment.

Tasks may include:

- Provide a customized SecOps ACC tab to view their threat landscape for a single PAN-OS Device user
- Configuration of up to five (5) EDLs to reduce time for incident mitigation
- Configuration of up to five (5) Log-Links for a single PAN-OS Device
- SecOps Log Profile remediation
- Review new features and their impact on SecOps
- Threat landscape assessment

- Create Daily/Weekly/Monthly reports for the SecOps to view the threat landscape on a single PAN-OS Device

2.4.3. On-site Event Analysis and Knowledge Transfer

A Palo Alto Networks consultant will perform event analysis and/or provide knowledge transfer for Client personnel, for a maximum of eight (8) hours per day for four (4) consecutive days. The topics reviewed and discussed are dynamic depending on configuration and relevant security events. Topics may include:

- How to view their current threat landscape via Application Command Center (ACC)
- Security Event Analysis Review
- Security Policy review and optimization
- Security Profile review and optimization, which may include:
  - Antivirus tuning recommendations
  - Anti-Spyware tuning recommendations
  - Vulnerability Protection tuning recommendations
  - URL Filtering recommendations
  - File Blocking tuning recommendations
  - WildFire configuration recommendations
- Zone Protection recommendations
- Custom Application/Application Override review and optimization
- Review of new features and their impact on SecOps
- How to mitigate bad actors quickly with the configured EDL security policies
- How Log-Links assists in the incident investigation
- Walkthrough of contextual information found in Palo Alto Networks services
  - Applipedia
  - Threat Vault

2.4.4. SecOps Solution Documentation

Palo Alto Networks will deliver SecOps Solution Documentation. This documentation will include the following:

- Recommended Changes Document - create a detailed document that describes policy and configuration recommendations provided during the engagement, and
- an Operations, Administration, and Management Guide for ongoing daily/weekly/monthly tasks
- As-Built Configuration document

Prior to final delivery, Palo Alto Networks will review the SecOps Solution Documentation with the Client team to incorporate Client-specific feedback.

2.5. Deliverables

PROJECT DELIVERABLES	
Project Deliverable	**Deliverable Criteria**
Planning and Qualification Document	Review Client Environment Review Client Environment team structure Review Client equipment catalog Client provided Tech Support File for the project scope(d) devices
SecOps Solution Documentation	Detailed document that describes policy and configuration recommendations provided during the engagement Operations, Administration, and Management Guide for ongoing daily/weekly/monthly tasks As-Built configuration document

2.5.1. Prerequisites, Assumptions, and Exclusions

2.5.1.1. Prerequisites

Prior to the delivery of the Services, Client will ensure that:

- Provide access to key team members as identified by Palo Alto Networks
- Assign a SecOps project resource
- Assign a SecOps team project resource to assist with scheduling and communication between the interfacing teams
- Assign a firewall change approval project resource
- Approve a change window for the Strata Cloud Manager, Log Collector, and Firewall
- Assign a Network Operations project resource with Administration access to PAN-OS Devices
- Assign a SecOps project resource with an understanding of their SIEM RESTful API
- A recent (less than two (2) weeks old) Tech Support File to be provided within one (1) week of engagement start for in-scope device

2.5.1.2. Assumptions

The following assumptions will apply to the Services:

- Client is responsible for any and all process changes
- Implementation of all recommendations will be performed by the Client as desired.

2.5.1.3. Exclusions

This is based upon, and is subject to, the following exclusions:

- No formal training manuals, workbook, lab guides, or other documents will be provided
- Deliverable is non-transferrable
- Knowledge transfer is limited to the Products and Services provided under this Service
- Any activities other than those explicitly defined

2.6. GlobalProtect Deployment

2.6.1. Deliverable Summary

Palo Alto Networks will deploy GlobalProtect remote access service and operationalize client for ongoing expansion and support as defined in the Information section.

2.6.2. Tasks and Activities

- Discovery
- Configure GlobalProtect Portals
- Configure GlobalProtect Gateways
- Assist with the deployment and configuration of Security rules to support the pilot
- Configuration of authentication
- Configuration of pilot GlobalProtect Agent profile(s)
- Support for pilot turn-up
- Knowledge Transfer Enablement of Client for ongoing support and growth
- As-built Documentation

2.6.3. Prerequisites, Assumptions, and Exclusions

2.6.3.1. Prerequisite

The following items are prerequisites before Palo Alto Networks will begin work on the Deliverable:

- The NGFW Platform is deployed and ready for configuration.
- Client has determined how they will deploy the GlobalProtect Agent to endpoints.
- Any required PKI elements in place.
- Any required licenses are installed and enabled.

2.6.3.2. Assumptions

The following are assumptions specific to this Deliverable:

- Client will be responsible for deploying the GlobalProtect Agents down to endpoint
- Client's Remote Access SME will be available during all configuration and deployment activities
- Client and Palo Alto Networks Consultant will determine testing criteria for completion signoff.
- Base configuration and documentation tasks will be performed remotely.

- Palo Alto Networks resources will follow the Client's change control process for the commitment of any production changes.

2.6.3.3. Exclusions

For the avoidance of doubt, the following items are excluded from the Deliverable scope:

- Palo Alto Networks Engineers will not rack, stack or cable devices.
- Palo Alto Networks Engineer is not responsible for deploying the agent down to the endpoint.
- Any activities not defined in the Tasks and Activities section.

2.7. Strata Cloud Manager

2.7.1. Deliverable Summary

Palo Alto Networks will, with Client's assistance, configure the Strata Cloud Manager management system(s) and Log Collector(s), as stated in the Information section, appropriate for the Palo Alto Networks Products in the Target Network. The Target Network Strata Cloud Manager may be configured as stand-alone or in High Availability Active/Passive mode. The Target Network Strata Cloud Manager will be configured to manage the in-scope NGFW(s) as defined in the Information section.

The Deliverable is the successful implementation of the Palo Alto Networks Strata Cloud Manager system with the baseline configurations as defined in the accepted Requirements (defined below) and outlined in the activity list in this section.

Palo Alto Networks will provide As-Built Documentation at the completion of the implementation activities defining the configurations used in the implementation of the Palo Alto Networks Products during this Deliverable.

2.7.2. Tasks and Activities

2.7.2.1. Technical Requirements Review

Palo Alto Networks will review, with Client, a Client-provided architecture, design and configuration of Legacy Network, and document the mutually agreed technical requirements (the "Requirements") for implementation into the Target Network. Requirements include:

- Validate the business and technical goals and objectives behind the Legacy Network and configurations, and apply as applicable to the Target Network configurations.
- Review Client network environment to identify any network or external dependencies that may interfere with the deployment.
- Strata Cloud Manager
  - If new Strata Cloud Manager, initial Strata Cloud Manager system configuration
  - Folders
  - Snippets/Stacks
  - Administrative authentication
  - Security profiles (visibility only) to be applied on the Target Network.
  - URL profiles (alert only) to be applied on the Target Network.
  - Intrusion prevention system settings, such as URL Filtering, Antivirus, Anti-Spyware, and Vulnerability Protection.
  - Logging profiles to be applied on the Target Network.
- Logging
  - Configure Log Collector(s)

2.7.2.2. Strata Cloud Manager Configuration and Review

Palo Alto Networks will work with the Client to configure the targeted Palo Alto Networks Strata Cloud Manager system(s) based on the mutually agreed upon Requirements. Palo Alto Networks will conduct a validation session with Client to verify the Strata Cloud Manager configuration before migration activities.

2.7.2.3. Logging Configuration and Review

Palo Alto Networks will work with the Client to configure the targeted Palo Alto Networks Log Collector configuration(s) based on the mutually agreed upon Requirements. Palo Alto Networks will conduct a validation session between Palo Alto Networks and Client to validate the logging configuration before migration activities.

2.7.3. Prerequisites, Assumptions, and Exclusions

2.7.3.1. Prerequisites

Client must complete the following items before Palo Alto Networks will begin work on the Deliverable:

- All purchased Palo Alto Networks Products (not demo/evaluation) are in a state of readiness for configuration.
  - If hardware appliance(s) are procured, all Palo Alto Networks hardware is racked, stacked, powered, and cabled.
  - If virtual appliance(s) are procured, all host system hardware/software is ready to accept virtual firewall image.
- All Palo Alto Networks Products are registered on the Palo Alto Networks support site.
- Provide Palo Alto Networks all applicable product license(s).
- Provide access to key team members as identified by Palo Alto Networks.
- Provide any identified information to Palo Alto Networks to facilitate the Requirements discussion and configuration planning.
- If requested by Palo Alto Networks, provide timely remote access, without charge, that includes the relevant Palo Alto Networks Products and any required testing equipment.

2.7.3.2. Assumptions

The following are assumptions specific to this Deliverable:

- Client is responsible for any and all configuration changes to any non-Palo Alto Networks products.
- PAN-OS software release recommendation will be based upon generally available hardware and software features as defined in the Requirements.
- Documentation will be provided in English.
- Documentation will be based on Palo Alto Networks snippet formats.

2.7.3.3. Exclusions

For the avoidance of doubt, the following items are excluded from the Deliverable scope:

- Installation of any and all hardware/software necessary for the implementation of the Services, including, but not limited to: all firewalls, servers, operating systems, networking equipment, cabling, and power.

- Security architecture and/or design services, other than what is required by Palo Alto Networks to develop the Requirements document.
- Configuration of any other Palo Alto Networks products not related to the target firewall or management system.
- Lab environment installation or preparation.
- Any activities not defined in the Tasks and Activities section.

2.8. Cloud Identity Engine (CIE) Implementation

2.8.1. Deliverable Summary

Palo Alto Networks will, with the Client's assistance, execute the implementation of the Cloud Identity Engine (CIE) solution for the NGFWs identified in the table below. The implementation will be done in accordance with the Client's change management process. All the work will be performed remotely.

The model and quantity information about the in-scope NGFWs and Strata Cloud Managers can be found in the Information section. It is assumed that the NGFWs are deployed in HA pairs and are managed by Strata Cloud Manager.

2.8.2. Tasks and Activities

- Discovery and Readiness Checks
- Configuration and Deployment of Directory Synchronization of seven (7) supported Directories
- Configuration and Deployment of Cloud Authentication Service of three (3) supported Identity providers
- Create and Deploy Cloud Identity Engine Configuration on the identified NGFWs and Strata Cloud Manager
- Configuration and Deployment of five (5) Cloud Authentication Profiles
- Configuration and Deployment of five (5) Authentication Policies
- Configuration and Deployment of five (5) Captive Portals
- Create/Update one (1) GlobalProtect configuration (applies only to authentication-related configuration)
- Create/Update ten (10) CIE Group-Based Security Policies
- Cutover and post-cutover support
- Knowledge Transfer Enablement of Client for ongoing support and growth. One (1) session is included in scope - four (4) hours max per session
- Creation of deployment plan, testing plan, and as-built documentation

2.8.3. Prerequisites, Assumptions, and Exclusions

2.8.3.1. Prerequisite

The following items are prerequisites before Palo Alto Networks will begin work on the Deliverable:

- The NGFWs are deployed with the appropriate PAN-OS version and ready for CIE configuration
- Client to identify and coordinate key team members who will be responsible for review and delivery of the solution.

- Provide access to key team members as identified by Palo Alto Networks for any follow-up and/or review activities.

2.8.3.2. Assumptions

The following are assumptions specific to this Deliverable:

- All tasks will be performed remotely unless otherwise stated
- Palo Alto Networks resources will follow the Client's change control process for the commitment of any production changes.
- Client will provide agreed-upon PAN-OS (and if applicable, Strata Cloud Manager) configurations to Palo Alto Networks for review and validation
- Proposed design is based on the Client accepting all recommendations
- All documentation will be provided in English

2.8.3.3. Exclusions

For the avoidance of doubt, the following items are excluded from the Deliverable scope:

- Full GlobalProtect deployment (The scope for this engagement is limited to the creation or updating of GlobalProtect CIE authentication-related configuration only)
- Operational support for the CIE solution
- Configuration and/or Method of Procedure guides
- Change Management process
- Any activities not defined in the Tasks section

2.9. App-ID Policy Conversion

The objective of this Service, to be agreed upon at Project kick-off, is to provide the Client with the expertise to:

- Remotely perform an App-ID conversion on an existing NGFW

Service Parameters

Parameter	In Scope	Description
Number of App-ID conversions	1	Perform an App-ID Policy Conversion on an existing Palo Alto Networks NGFW - two cutover events included.
Number of NGFWs	1	One single or one Active/Passive HA pair of NGFWs
Number of Security Rules to convert and review	100	Convert and review up to (100) Security Rules from protocol/port-based to App-ID-based rules.

2.9.1. Discover

Palo Alto Networks will review with the Client the requirements to convert up to (100) Security Rules from protocol/port to App-ID on one (1) NGFW currently being deployed or in production. Palo Alto Networks will work with the Client to identify the target rules, based on their prioritization, and review the conversion process. This will be used to capture the mutually agreed technical requirements (the "Requirements") for implementation of the new capability.

Palo Alto Networks will provide a predefined Technical Requirements Document ("TRD"), as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific requirements. The final TRD will be mutually agreed upon prior to moving to the next phase of the project.

2.9.2. Configure and Review

Palo Alto Networks will work with the Client to configure the targeted Palo Alto Networks device based on the mutually agreed-upon Requirements.

2.9.3. First Pass

Palo Alto Networks will review the configuration and the App-ID converted rules with the Client team before the production deployment event to validate the accuracy of the NGFW configuration. This time must be scheduled in advance and in a single four (4) hour session.

2.9.4. Second Pass

Palo Alto Networks will review the NGFW Traffic Logs for the App-ID converted rules with the Client team after the initial production deployment event to verify App-ID functionality and tune the previously converted App-ID Security Rules. This time must be scheduled in advance and in a single four (4) hour session.

Palo Alto Networks will provide a predefined Deployment Playbook and Validation Plan, as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific requirements and feedback. The final Deployment Validation Plan will be mutually agreed upon prior to moving to the next phase of the project.

2.9.5. Production Deployment

Palo Alto Networks will assist the Client in performing two (2) production deployment events of up to four (4) hours each, scheduled during or after business hours. The purpose of this will be to introduce the App-ID capability into the Client environment after the initial App-ID conversion/review and again after the App-ID review/tuning, as defined under Configure and Review.

Post introduction, Palo Alto Networks will assist with verification of functionality and troubleshooting any production issues related to introducing App-ID. If required, the Consultant will assist the Client and the Palo Alto Networks Technical Assistance Center ("TAC") to raise cases as needed.

2.9.6. Knowledge Transfer

Palo Alto Networks consultant will provide up to four (4) hours of knowledge transfer. This time must be scheduled post-production deployment, in advance, and in sessions two (2) hours in length at a minimum.

2.9.7. Documentation

Palo Alto Networks will provide a predefined As-Built Configuration, as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific feedback.

2.9.8. Deliverables

The following Deliverables will be provided in accordance with the Services:

PROJECT DELIVERABLES	
Project Deliverable	**Deliverable Criteria**
Project Plan	Capture project management requirements Milestones Task/activities Owners Timeline
Technical Requirements Document (“TRD”)	Capture foundational configuration requirements Target NGFW for App-ID conversion Target Security Rules for App-ID conversion Establish a timeline for the Client to provide required information
Deployment Playbook* - based on TRD * Client to develop their own deployment plan	Capture production deployment requirements Production change event timing Production change event success and roll-back criteria Palo Alto Networks steps for deployment and roll-back
Deployment Validation Plan* - based on TRD * Client to develop their own application-specific test plan	Capture production deployment testing requirements Verification of configured functionality per TRD Identification of critical applications/flows - as provided by the Client Key Client testing/support resources for critical applications/flows
As-Built Configuration Document	Document the “as implemented” configuration of the deployed NGFW(s)

2.9.9. Prerequisites, Assumptions, and Exclusions

2.9.9.1. Prerequisite

The following items are prerequisites before Palo Alto Networks will begin work on the Deliverable:

- All purchased Palo Alto Networks NGFWs and/or Panorama are in a state of production readiness for the App-ID configuration.
- Identification of key Security Rules to be converted.

2.9.9.2. Assumptions

The following assumptions will apply to the Services:

- All implementation activity will follow Client's change control processes, as coordinated by Client's SPOC.
- Client will develop their own application test plan and facilitate appropriate testers/support personnel for the production deployment event.
- Palo Alto Networks will work with the Client to integrate into the existing networking environment within the limitations of the Product. Any changes to non-Palo Alto Networks systems in this environment are the responsibility of the Client.

2.9.9.3. Exclusions

This Service Description is based upon, and is subject to, the following exclusions:

- Security architecture or design services and/or documentation.
- App-ID Security Policy Conversion for:
  - More than one (1) NGFW or virtual system.
  - More Security Rules than identified under Service Parameters.
- Creation of custom App-ID(s).
- Redeployment of Palo Alto Networks products due to hardware sizing of the original purchase.
- Development of Client-specific Application Test Plan.

2.10. SSL Decryption

2.10.1. Deliverable Summary

Palo Alto Networks will assist in the deployment and development of SSL Decryption. Palo Alto Networks will create the SSL Decryption Profile(s) and deploy SSL Decryption policy(s) for high-risk categories as defined in the Information section.

- Enable SSL Decryption policy per select Palo Alto Network devices.
- Confirmation of actively encrypting SSL traffic via the Monitor tab of defined categories.
- Palo Alto Networks to deploy Decryption-defined categories.

2.10.2. Tasks and Activities

- Review meeting with Client to determine SSL Decryption policies for implementation.
- Create an SSL Decryption policy for agreed high-risk categories.
- Create an SSL Decryption Profile to handle exceptions.
- Test SSL Decrypt policy for deployed Categories.
- Provide knowledge transfer to Client for the implementation of additional SSL Decryption categories beyond the initially defined categories.

2.10.3. Prerequisites, Assumptions, and Exclusions

2.10.3.1. Prerequisites

The following items are prerequisites before Palo Alto Networks will begin work on the Deliverable:

- Acceptance of the previous Deliverables in this Statement of Work.
- Client has a PKI environment and has created and deployed trust for CA or sub-CA to all endpoints.
- Client provides all required security certificates.
- User-ID and PAN-DB deployed and operational prior to creating the SSL Decryption policy.

2.10.3.2. Assumptions

The following are assumptions specific to this Deliverable:

- Palo Alto Networks will develop and deploy initial SSL Decryption policies as defined in the HLD.
- Additional SSL Decryption policies beyond those defined in the HLD will be developed by the Client.
- Decryption policies may be limited by the perimeter hardware capabilities, that is, CPU and processing power.
- Documentation will be provided in English.
- Documentation will be based on Palo Alto Networks template formats.

2.10.3.3. Exclusions

For the avoidance of doubt, the following items are excluded from the Deliverable scope:

- Decryption of “all URL Categories”.
- Any activities not defined in the Tasks and Activities section.

2.11. Threat Prevention

The objective of this Service, to be agreed upon at project kickoff, is to provide the Client with the expertise to either:

- Remotely review existing Security Profile Groups, or
- Remotely create new Security Profile Groups

2.11.1. General

Parameter	Description
Target System(s)	The target system must be one of: Strata Cloud Manager, VM, or PA-Series NGFW.
Target Subscriptions	Threat, Advanced Threat, WildFire, and DNS Security - ***must*** have active license(s)

Parameter	Description
Target PAN-OS Version(s)	Generally available version of PAN-OS - Advanced Threat ***requires*** 10.2.0 minimum.

2.11.2. Review

Parameter	In Scope	Description
Number of Security Profile Groups	3	Review up to (3) existing Security Profile Groups against best practices
Number of NGFWs or Strata Cloud Manager Folders	5	Apply updated Security Profile Groups to all Security/NAT rules for up to five (5) target Palo Alto Networks NGFWs or Strata Cloud Manager Folders - one cutover event included

2.11.3. Create

Parameter	In Scope	Description
Number of Security Profile Groups	3	Create up to (3) new Security Profile Groups using best practices
Number of NGFWs or Strata Cloud Manager Folders	5	Apply new Security Profile Groups to all Security/NAT rules for up to (5) target Palo Alto Networks NGFWs or Strata Cloud Manager Folders - one cutover event included

2.11.3.1. Planning

Palo Alto Networks will, with Client's participation, conduct planning activities and a project kick-off call. The project kick-off will include a review of the project requirements (review or create), discuss milestone timelines, identify the Client's project team members, and follow-up action items.

Palo Alto Networks will provide a predefined Project Plan, as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific requirements/feedback. The final Project Plan will be mutually agreed upon prior to moving to the next phase of the project.

2.11.3.2. Discover

Review

Palo Alto Networks will review up to three (3) existing Security Profile Groups, already applied to existing NGFW Security/NAT rules, with the Client team and provide recommendations based on best practices. Palo Alto Networks will work with the Client to identify up to five (5) NGFWs or Strata Cloud Manager

Folders to apply the updated Security Profile Groups to. This will be used to capture the mutually agreed technical requirements (the “Requirements”) for updating the existing Security Profile Groups.

2.11.3.3. Create

Palo Alto Networks will assist the Client with identifying requirements for the creation of up to three (3) new Security Profile Groups. Palo Alto Networks will work with the Client to identify up to five (5) NGFWs or Strata Cloud Manager Folders to apply the new Security Profile Groups to. This will be used to capture the mutually agreed technical requirements (the “Requirements”) for creating the new Security Profile Groups.

Palo Alto Networks will provide a predefined Technical Requirements Document (“TRD”), as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific requirements. The final TRD will be mutually agreed upon prior to moving to the next phase of the project.

2.11.3.4. Configure and Review

Palo Alto Networks will work with the Client to configure the targeted Palo Alto Networks device(s) based on the mutually agreed upon Requirements.

Palo Alto Networks will provide a final review prior to the production deployment event to validate the accuracy of the Security Profile Group configuration. This time must be scheduled in advance and in a single two (2) hour session.

Palo Alto Networks will update the existing or provide a new predefined Deployment Playbook and Validation Plan, as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific requirements and feedback. The final Deployment Playbook and Validation Plan will be mutually agreed upon prior to moving to the next phase of the project.

2.11.3.5. Production Deployment

Palo Alto Networks will assist the Client in performing one (1) production deployment event scheduled during or after business hours. The purpose of this will be to introduce the updated or new Security Profile Groups capability into the Client environment.

Post introduction, Palo Alto Networks will assist with verification of functionality and troubleshooting any production issues related to introducing Threat prevention. If required, the Consultant will assist the Client and the Palo Alto Networks Technical Assistance Center (“TAC”) to raise cases as needed.

2.11.3.6. Knowledge Transfer

Palo Alto Networks consultant will provide up to two (2) hours of knowledge transfer. This time must be scheduled post-production deployment, in advance, and in a single two (2) hour session.

2.11.3.7. Documentation

Palo Alto Networks will update an existing or provide a predefined As-Built Configuration, as defined under Deliverables, and perform one (1) review with the Client team for the addition of Client-specific feedback.

2.11.4. Deliverables

PROJECT DELIVERABLES	
Project Deliverable	**Deliverable Criteria**
Project Plan	Capture project management requirements Milestones Task/activities Owners Timeline
Technical Requirements Document (“TRD”)	Review Capture foundational configuration requirements Security Profile Groups to be reviewed Subscription(s) available to configure NGFWs or Folders to update Establish a timeline for the Client to provide the required information Create Capture foundational configuration requirements Security Profile Groups to be created Subscription(s) available to configure NGFWs or Folders to apply to Establish a timeline for the Client to provide the required information
Deployment Playbook - based on TRD	Capture production deployment requirements Production change event timing - if required Production change event success and roll-back criteria Palo Alto Networks steps for deployment and roll-back
Deployment Validation Plan - based on TRD	Capture production deployment testing requirements Verification of configured functionality per TRD

As-Built Configuration Document	Document the “as implemented” configuration of the deployed functionality

2.11.5. Prerequisites, Assumptions, and Exclusions

2.11.5.1. Prerequisite

Prior to the delivery of the Services, Client will ensure that:

- All purchased Palo Alto Networks Products (not demo/evaluation) are in a state of readiness for configuration (racked, stacked, powered, cooled, and cabled).
- All Palo Alto Networks Products are registered on the Palo Alto Networks support site.
- All Palo Alto Networks licenses/activation codes are available to be utilized.
- All Palo Alto Networks systems are at the required version of PAN-OS.

2.11.5.2. Assumptions

The target NGFWs and/or Strata Cloud Manager are in production or being deployed via an existing deployment project.

All implementation activity will follow the Client’s change control processes, as coordinated by the Client’s SPOC.

2.11.5.3. Exclusions

This Service Description is based upon, and is subject to, the following exclusions:

- PAN-OS upgrades to support functionality.
- Security architecture or design services and/or documentation.
- Configuration of parameters for unlicensed capabilities.
- Configuration of new or review of existing Security Profile Groups beyond parameters identified in Service Parameters.
- Redeployment of Palo Alto Networks products due to hardware sizing of the original purchase.

3. ENGAGEMENT INFORMATION

3.1. Resources

Presidio approaches project execution from a skills-based perspective. Our Execution Team comprises individuals with specific skill sets that will be utilized at different times during a given project. This enables us to provide a highly specialized workforce to the Client and utilize the appropriate resources for the required task. The Project Manager or Project Coordinator will distribute contact information for the project team personnel.

The following Presidio resources will be engaged in this project:

Resource Name	Discipline
Engineer - 3rd party Sub Resource	Network Security

3.2. Locations

All services outlined in this SoW will be performed and delivered remotely unless otherwise specified. Services described in this SoW may be performed or will impact the following locations.

Location	Address	City State ZIP
FCG - Fulton County Government	141 Pryor St	Atlanta, GA 30303-3444

3.3. Outcomes and Deliverables

Documentation may be created by Presidio and provided as part of the Project Deliverables. Some of these deliverables may be delivered as a single document. The specific documentation to be provided depends on your chosen solution(s).

Client's acceptance of all deliverables described in this SOW and of the completion of the project shall be in writing. Deliverable acceptance shall be in the form of an email or signature (as applicable), and final project acceptance shall be in the "Project Completion Signoff" form provided by the Project Manager or Project Coordinator. If acceptance is refused, the Client shall provide, in writing to Presidio, a reason for refusal. Presidio shall address the issue before subsequent work is undertaken.

For any documentation provided, it shall be reviewed and approved by the Client in accordance with the following procedure:

- If a written list of requested changes is received within five (5) business days, the Presidio Project Team will make the agreed-upon revisions and resubmit the updated version to the client within five (5) business days.
- At that time, the Client has five (5) business days to review and request changes for the final document. If no written response is received from the Client within five (5) business days, either accepting or requesting changes, then the deliverable material shall be deemed accepted.
- Deliverables noted in appropriate section.

3.4. Technical Support after Completion

For non-critical support, including system expansion options, assessments, audits, and related services, or services that are not covered by a support contract with Presidio or another vendor, Presidio offers a variety of options, including Fixed Fee, Hourly Rate, or Daily Rate options. Pricing for these services is not included in this Statement of Work.

Managed Services Clients	Non-Managed Services Clients
Technical support for the solution implemented within the scope of this SOW can be obtained by: calling 800-494-0118, sending an email to presidio@service-now.com	Vendor's (such as Cisco or EMC) Support Center or Technical Assistance Center (TAC) is the vehicle for all support. These Vendor Support Centers provide 7x24 support on all hardware and software, including replacement parts, software patches and updates, and configuration assistance.

4. ASSUMPTIONS & RESPONSIBILITIES

Presidio makes the following assumptions and has identified the following Client responsibilities in developing this Statement of Work. These assumptions and responsibilities serve as the foundation on which the project estimate, approach, and timeline were developed. By signing this SOW, Client agrees that these assumptions and responsibilities are correct and valid. Any changes to the following assumptions and responsibilities must be processed using the Presidio Change Management Process and may impact the project duration and labor requirements.

4.1. Engagement Assumptions

The following project assumptions are made and will be verified as part of the engagement:

- Client has read and agrees with all Items contained or omitted within this Statement of Work.
- This SOW supersedes all prior written or oral agreements, representations, and understandings related to the subject matter hereof. Any purchase order submitted pursuant to this SOW shall be subject to the terms herein and shall not be subject to any new or different terms, including pre-printed terms on such order. All changes to this SOW must be executed in writing and accepted by both parties, as indicated by authorized signature, prior to the execution of work.
- Presidio will hold no responsibility for any changes made "after" releasing the system to the Client. Presidio expressly disclaims any liability for non-performance or the delivery of poor quality of services resulting from errors or omissions in information provided to Presidio by Client, whether Presidio knew or should have known of any such errors or omissions, or whether Presidio was responsible for or participated in the gathering of such information. Significant delays, revisits, or cancelled changes outside of Presidio's control may necessitate a change order to account for rescheduling.
- Working Hours: Presidio and Client will jointly agree on the location of the resources, onsite requirements, and what time the services will be provided. By default:
    - Services delivered by resources working in North America and Europe will be provided from 8 AM to 5 PM, relative to the local time zone of the assigned resources, Monday through Friday, excluding standard Presidio holidays specific to the resources' location.
    - Services delivered by resources working in India will be provided from 11 AM to 8 PM IST, Monday through Friday, excluding standard Presidio holidays specific to the resources' location.
    - Resources may work hours other than those defined as normal business hours to accommodate their travel schedules and time zones.
- Any Items or tasks not explicitly listed as in-scope within this SOW are considered to be outside of the scope and not associated with this SOW and price.
- If integration of the product is performed at a Presidio facility, then transfer of ownership (acceptance) occurs upon the receipt and integration of goods at Presidio, regardless of shipment, as manufacturers will not accept returns of opened products.
- Presidio will not be responsible for troubleshooting networks, applications, and/or hardware if the Client does not have formal change management documented processes and policies.
- Presidio may engage subcontractors and third parties in performing a portion of this work.
- Presidio will not make changes to the configuration of any network equipment after it has been installed and tested.
- Some activities included in this project may be performed on Presidio's premises.
- Not all features or functions of the installed system are included in the scope of this engagement.

- Presidio reserves the right to modify the approach outlined within this SOW if it does not alter the timeline or overall outcome of the engagement.
- Presidio will configure the systems outlined within this Statement of Work with a unique set of authentication credentials unless otherwise provided by the Client. Upon the completion of the engagement, Presidio will provide Client with all usernames, passwords, and additional authentication information that were implemented during the engagement. Presidio strongly recommends that these credentials be changed upon the completion of the engagement.
- Any documentation will be delivered in Presidio format unless otherwise stated in this SOW.
- Project success criteria will be defined by the Client and jointly agreed to with Presidio.
- Client staff will participate throughout the implementation.

4.2. General Client Obligations, Assumptions, and Exclusions

Successful and timely completion of the Services is subject to Client meeting its obligations under this SOW, and Palo Alto Networks shall not be responsible for any delay due to Client's non-compliance with its obligations.

Client Obligations

Prior to the delivery of the Services, Client will:

- Provide a project manager or other single point of contact ("SPOC") for the project who will be responsible for:
  - Providing all information, as requested by Palo Alto Networks, in a timely manner in order for Palo Alto Networks to consistently achieve the Services in the timeframe for each Deliverable.
  - Acting as the central point of contact to Palo Alto Networks.
  - Coordination of Client resources engaged in the project. Client's technical resources should be qualified on Palo Alto Networks Products.
- Be responsible for the procurement of any and all licenses for the Palo Alto Networks Products and provide to Palo Alto Networks professional services consultant(s) upon request.
- Provide Palo Alto Networks professional services consultant(s) with existing and up-to-date documentation, including, but not limited to: topological diagrams, design documentation, up-to-date configurations, and change management policy documentation.
- Advise Palo Alto Networks of any:
  - Special security, health, and safety matters applicable.
  - Relevant project management meetings related to the project and/or Services, and permit Palo Alto Networks to attend such meetings as appropriate.
- Be responsible for managing all other vendors, including, if applicable, Client's managed services partner or systems integrator.
- Be responsible for any and all configuration changes to any non-Palo Alto Networks Products.
- Provide prompt written notice to Palo Alto Networks as soon as Client becomes aware or has reason to believe that: Client will not meet any of the Client obligations under this Client Obligations section, and/or if any of Palo Alto Networks assumptions will not occur or are inaccurate.
- Provide any additional equipment, such as network analyzers, test equipment, and/or laboratory equipment that are not provided by Palo Alto Networks, but are necessary to perform the Services.

- Ensure that Palo Alto Networks personnel may access and use Client's and third-party licensors' proprietary materials as necessary for Palo Alto Networks to perform the Services. Client warrants and represents that it has the right and authority to grant such access and use to Palo Alto Networks and hereby grants Palo Alto Networks the rights to use and access such proprietary materials as needed for Palo Alto Networks to perform the Services.

Assumptions

Throughout the delivery of the Services, Client will:

- Upon request or as needed, Client shall provide access to the skilled subject matter and technical experts within Client's (or their third-party vendor) organization for Palo Alto Networks to perform the Services.
    - Perform all responsibilities and obligations specified under this Service in a professional workmanlike manner to facilitate the timely completion of the Services.
- Provide direct remote access to the Palo Alto Networks equipment to be worked on via a Palo Alto Networks-owned laptop.
    - Where direct remote access cannot be provided to Palo Alto Networks-owned laptops, Client shall provide alternative laptops with appropriate capabilities and connectivity, or other functionally equivalent connectivity.

Exclusions

This Service is based upon, and is subject to, the following exclusions:

- The Services will not commence until Palo Alto Networks has received a non-cancellable PO for the Services.
- Palo Alto Networks is responsible for providing only the Services with the associated Deliverables described in this Service. Palo Alto Networks shall have no responsibility for other contractors or third parties engaged by Client or another third-party during delivery of the Services unless expressly agreed to in writing.
- Palo Alto Networks shall not be responsible for any delays caused by the Client or any third party.
- Services are non-transferable.

4.3. Client Responsibilities

The following Items are listed as the Client's responsibilities for this engagement. Client is responsible for performing the Items and activities listed in this section or arranging for them to be performed by a third party if appropriate.

- Provide a primary contact and a secondary contact when the primary is unavailable with the authority and the responsibility of issue resolution, and the identification, coordination, and scheduling of Client personnel to participate in the implementation of the SOW. Without a single Client point of contact, a Project Change Request may be required for the additional effort by Presidio.
- Be responsible for having in place active manufacturer support contracts on all devices that are the subject of this SOW.
- If on-site services are required and authorized, Client will:
    - Provide all required physical access to Client's facility (identification badge, escort, parking decal, etc.), as required by Client's policies.
    - Validate the site readiness prior to the dispatch of Presidio personnel to perform the services being contracted.
- If system access is required:

- Provide all required functional access (passwords, IP address information, etc.), as required for Presidio to complete the tasks.
- Provide high-speed access to the Internet for verification of device support requirements and for software downloads.
- Provide VPN remote access for troubleshooting and configurations related to the project, as necessary. Utilizing Webex, Microsoft Teams, or other similar screen-sharing/meeting technology as opposed to independent VPN access or virtual desktop is out of scope. If there is no other option, Presidio will issue a Change Request to add additional funds to the project to accommodate the increase in time and effort.

- Provide required and requested documentation or information needed for the project within two (2) business days unless otherwise agreed to by all parties.
- Provide Presidio with access to their systems, appropriate processes, and personnel as reasonably necessary for Presidio to fulfill its obligations.
- Where appropriate, knowledgeable resources will be made available for functional questions and making business decisions. It is also expected that Client staff will participate throughout the implementation.
- Participate in all working sessions as required to produce the success and efficacy of the services rendered.
- The Services must be delivered within six (6) months from the SOW Effective Date. Any Services remaining following this period will expire, along with any obligation to deliver any further Services unless otherwise mutually agreed to in writing.

5. PRICING

Presidio will provide the services outlined in this Statement of Work for a fixed fee of **$282,591.92**.

Description	Amount
Project SOW Signing	$282,591.92
Total	**$282,591.92**

- Presidio will bill Client upon signing of this Statement of Work.
- If Client delays the project start or delays work on a subsequent milestone, Client must give Presidio written notice of delay no less than two (2) weeks before work was scheduled to begin. If Client does not give adequate notice of the delay, Client may be liable to pay an amount equal to the milestone to be delayed based on the Project Pricing section.

5.1. Additional Expenses

There is minimal travel included in the pricing. If more travel to the Client's facility is requested and authorized by the Client, then all authorized, reasonable travel and expenses will be reimbursed to Presidio at an actual cost within 30 days of submission of an invoice to the Client.

6. APPROVAL SIGNOFF

The use of signatures on this Statement of Work ensures agreement on project objectives and the work to be performed by Presidio.

Presidio's signature signifies our commitment to proceed with the project as described in this document. Please review this document thoroughly, as it will be the basis for all work performed by Presidio on this project.

This Statement of Work is valid for a period of 60 days from the date that this Statement of Work is provided by Presidio to Client unless otherwise agreed to by both parties.

FCG - Fulton County Government

Signature	Date mm-dd-yyyy
Printed Name	Title

PRESIDIO

Signature	Date mm-dd-yyyy
Printed Name	Title