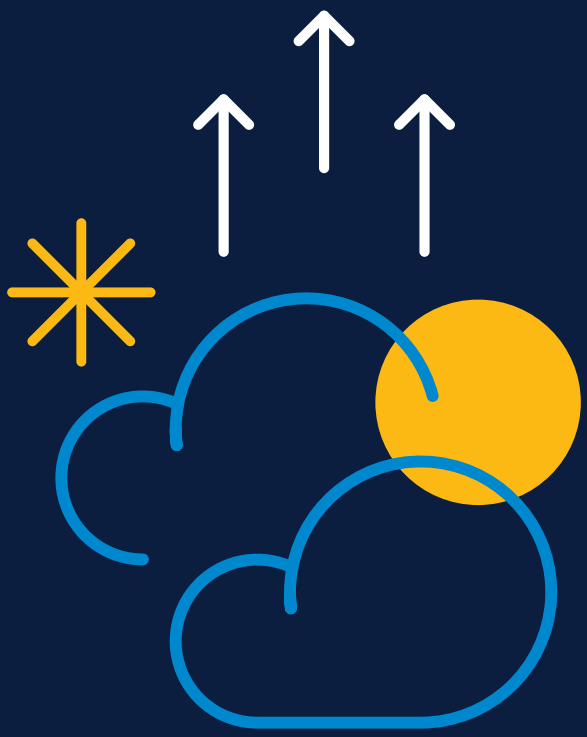
US SIGNAL®

Palo Alto

CUSTOMER GUIDE



WELCOME TO US SIGNAL'S MANAGED SECURITY OFFERING FOR CLOUD BASED ADVANCED SECURITY (CBAS)

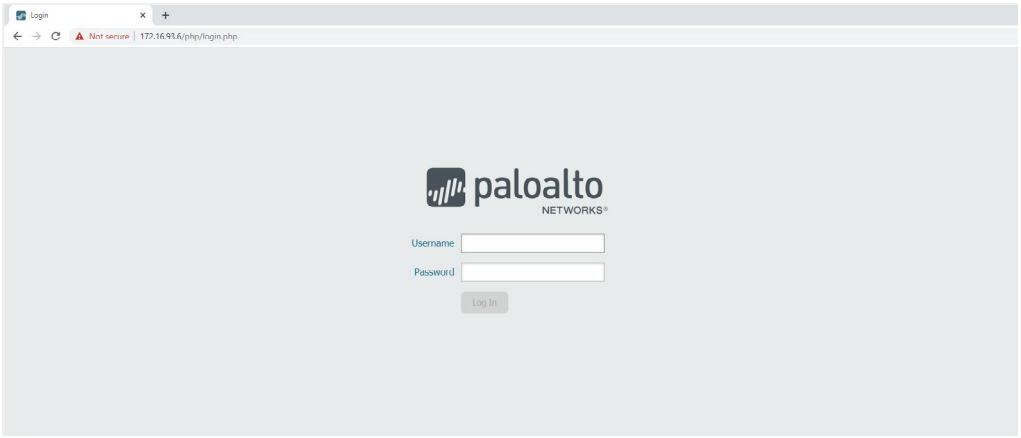
As a valued customer, you will have read-only access to your CBAS firewall dashboard. This will streamline operation and communication when working with our Technical Operations Center (TOC). This is a managed product, so please contact the US Signal TOC regarding the use or configuration of features.

Please note, for an improved security posture and to align with best practices, the dashboard is only accessible from your local area network (LAN) behind the firewall.

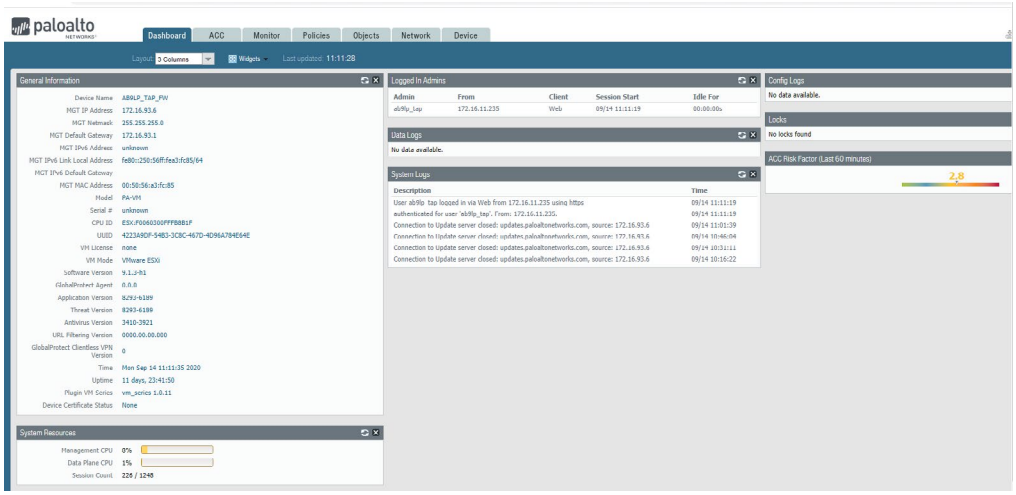
The US Signal TOC can be reached at 888-663-1700, 24 hours a day, 365 days a year.

ACCESSING THE FIREWALL

+ Your US Signal Project Manager will provide you all necessary login information upon order completion.
+ To access your CBAS, you will need to use any computer within your LAN.
+ In a web browser (we recommend Chrome), navigate to the URL bar, and enter the IP address of your CBAS appliance. See the example below:



+ Upon successful authentication, you will be logged in to the main dashboard of the CBAS firewall. From the dashboard, you can freely navigate to view settings and security policies. Any questions or requests can be directed to the US Signal TOC.



NAVIGATING THE FIREWALL

Once logged in, you will see the following tabs at the top of the session. Each provides access to various features of the Palo Alto firewall.

+ **Application Command Center (ACC):** The ACC is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing your network.
+ **Monitor:** View logs, current sessions, and generate reports.
+ **Policies:** View Security and NAT policies.
+ **Objects:** View objects for IP addresses, Applications, URL Lists, and IDS/IPS profiles.
+ **Network:** View interfaces, route tables, and Site-to-Site/Remote Access VPN properties.
+ **Device:** View local users and multi-factor profiles.

KEY FEATURES OF THE FIREWALL

One of the biggest features of the CBAS is the ability to control traffic, not only by source/destination IP address and port, but also by application. Applications are identified based on traffic patterns and restrict traffic to only known ports. US Signal recommends using default port(s) on the application wherever possible but understands this cannot always be accomplished. The TOC can and will work with you on moving towards a better security posture as you see fit to harness the full capabilities of the Palo Alto Firewall.

The CBAS has a robust IDS\IPS solution that can be fully customized to meet the demands of your environment. Below is a breakdown of each profile that can applied per rule to achieve increased security.

Antivirus
+ Detects infected files being transferred within the application.
+ Scans for Malware, Worms, and Viruses while downloading files.
+ The default profile inspects all listed protocol decoders for viruses and generates alerts for SMTP, IMAP, and POP3 protocols while blocking FTP, HTTP, and SMB protocols.

Anti-Spyware
+ Detects spyware downloads and traffic from already installed spyware.
+ Blocks spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus allowing you to detect malicious traffic leaving the network from infected clients.

Vulnerability Protection
+ Detects attempts to exploit known software vulnerabilities.
+ Stops attempts to exploit system flaws or gain unauthorized access to systems.
+ Typically used to stop threats coming into the network related to buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

URL Filtering
+ Classifies and controls web browsing based on content.
+ Determines web access permissions for each URL category.
+ Ability to create custom URL categories and URL lists for more granular control.

File Blocking
+ Tracks and blocks file uploads and downloads based on file type and application.
+ Blocks selected file types from being uploaded/downloaded or generates an alert when the specified file types are detected.

Data Filtering
+ Identifies and blocks transfer of specific data patterns found in network traffic.
+ Used to prevent sensitive, confidential, and proprietary information from leaving your network.
+ Data patterns are used to define the information types that you want the firewall to filter.

Wildfire Analysis
+ Forwards unknown files to the Wildfire® service for malware analysis.
+ Cloud-based virtual sandbox used to evaluate unknown files and URL links found in emails.

REMOTE ACCESS VPN

+ Global Protect is an agent-based VPN solution allowing end users to connect to your LAN effortlessly from anywhere. This has a slew of customizations built into it to meet the requirements of your business security posture.
  https://docs.paloaltonetworks.com/compatibility-matrix/globalprotect/what-features-does-globalprotect-support

BEST PRACTICES AND TIPS

+ Collection of vendor recommended best practices for a Palo Alto Firewall:
  https://docs.paloaltonetworks.com/best-practices

+ All applications on a Palo Alto firewall. Search by name, category, or port number:
  https://applipedia.paloaltonetworks.com/

+ Frequently used applications for day to day operations:
  + **Web-browsing** – This is equal to port 80 or HTTP traffic.
  + **SSL** – This is equal to port 443 or HTTPS traffic.
  + **Ms-update** – This is used for Windows\Microsoft updates.
  + **Ms-office365** – This is used for access to Office 365 applications.
  + **SMTP** – This is equal to port 25 and used for SMTP mail traffic.