US SIGNAL MANAGED SECURITY: CBAS PALO ALTO FEATURE INFORMATION SHEET

US Signal's core Managed Security service, CBAS, is powered by Palo Alto for the best zero-trust and threat intelligence in the industry. The goal of this document is to provide clear and concise information relating to the CBAS feature set and what is supported in the US Signal environment.

VM-Series Firewalls & Sizing

US Signal takes advantage of Palo Alto's VM-series Palo Alto firewalls and deploys them in our managed data centers. For many customers, these firewalls provide access to the Internet for various cloud and MPLS services. These firewalls also provide a Site-to-Site and Remote Access VPN termination point to connect to remote customer branch offices.

These firewalls are licensed in tiers that dictate capabilities and limitations. The most significant limitation to be aware of is the amount of bandwidth the firewall is capable of processing. Firewalls that have the Intrusion Detection/ Prevention (IDS/IPS) component enabled will be limited to half of the maximum bandwidth. Please refer to the image below.

Firewall Sizing Table	VM 50	VM 100	VM 300
With IDS and IPS Turned On	50 Mbps	500 Mbps	1 Gbps
Without IDS and IPS Turned On	100 Mbps	1 Gbps	2 Gbps

For this reason, it is important to select a licensing tier that meets the customer's requirement.

A full list of capabilities for each VM-Series model can be found by clicking **here**.

Note: US Signal does not offer any of the "Lite" licensed tiers.

Firewall Management

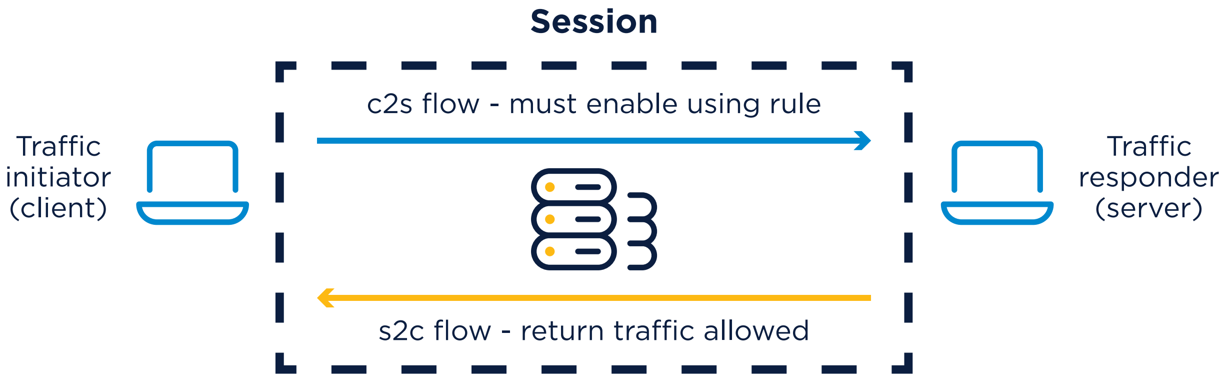
The Palo Alto firewall, by default, is setup as a zero-trust platform. This means that all inbound and outbound network traffic will be blocked unless a security policy rule explicitly permits it. Customers will gain read-only access to the firewall by accessing the web GUI via HTTPS from within the internal LAN. This allows the customer to view traffic and threat logs, review security and NAT policy rules, monitor VPN status and generate reports.

Customers that require changes to the firewall must generate a trouble ticket with the Technical Operations Center (TOC) by calling in or sending an email and referencing the firewall's unique Circuit ID. The TOC support team is trained to handle modifications to the firewall in addition to configuring new features supported by the firewall platform.

Firewall Traffic Flow

The Palo Alto is a stateful firewall, where the firewall builds a session composed of two unidirectional traffic flows (Client-to-Server and Server-to-Client) when a security policy rule permits traffic. This session allows the firewall to automatically allow return traffic back to the firewall without the need of creating an additional security policy rule.

When making security policy rule requests, you must consider only the Client-to-Server traffic flow. That is: “Where is the traffic originating from, and where is the traffic going to”. The return traffic generated from the responder, or destination host, will be allowed in without the need for a security policy rule.


Session
c2s flow - must enable using rule
Traffic initiator (client)
Traffic responder (server)
s2c flow - return traffic allowed

Application Filtering (App-ID)

The Palo Alto firewall features Layer 7 (application) filtering on network traffic when processing security policy rules. Traditional legacy firewalls process network traffic based on Source/Destination IP address, Source/Destination ports, and transport layer protocol (TCP/UDP). This may allow for evasive and malicious applications to disguise themselves as “trusted” network traffic by using well-known ports and protocols.

The use of App-ID allows for the underlying application behind the network traffic to be identified and for security policy rule enforcement to take place based on the application. This is achieved by adding an extra layer of inspection that analyzes application signatures, heuristics, and protocol decoding on top of IP addresses, ports, and protocols.

Using the App-ID feature is implemented on a per security rule basis. While this does provide additional security benefits it can also inadvertently block network traffic that may be using non-standard ports, have unusual characteristics, or have custom application signatures. It is recommended to utilize application-level filtering on security policy rules only when a there is a clear understanding on which applications are in use within a customer’s unique environment.

For a full list of applications that are recognized by the Palo Alto firewall, please refer to the following link **here**.

Note: This application database is automatically updated with new applications every month, and modifications to existing applications are made weekly.

Site-to-Site VPN

The Palo Alto firewall utilizes a route-based VPN solution where encrypted traffic is forwarded over a virtual tunnel interface based on destination IP address. The main benefits of implementing a route-based VPN solution are that it allows for dynamic routing to occur over a VPN connection and it allows for dynamic failover between primary and backup VPN tunnels.

Fortunately, the Palo Alto firewall can interoperate with third-party firewalls that utilize a policy-based VPN solution. It is important to understand that while interoperating with a third-party policy-based VPN, the benefits of dynamic routing and VPN failover are limited. Depending on the vendor, these benefits may not be supported at all. It is recommended to work with the customer to determine whether Site-to-Site VPNs will be a requirement, which firewall vendor(s) they have supporting their remote branches, and whether their vendor supports a route-based VPN solution.

The biggest limitation with route-based VPN solutions is when there are overlapping remote VPN subnets. Since the Palo firewall forwards traffic over a VPN tunnel based on its routing table, there cannot be overlapping destination networks between different VPN tunnels.

Remote Access (Client-Based) VPN

The Palo Alto firewall's Remote Access client-based VPN solution is referred to as GlobalProtect. This allows mobile/remote users to gain access to their company's internal resources maintained in US Signal's infrastructure.

By accessing the Fully Qualified Domain Name (FQDN) of the Palo Alto firewall from a web browser, the customer can download the GlobalProtect client and configuration file on their local machine. Mobile users can download the application from the iOS/Android App store and similarly navigate to the firewall's FQDN to obtain the configuration file.

To authenticate remote VPN users, it is recommended that the customer provides an external authentication source, such as an LDAP or RADIUS server. This allows the customer to maintain complete control over account administration. However, the customer can alternatively use the Palo Alto's local user account database as an authentication source. When using local authentication, the customer is responsible for contacting the Technical Operations Center to create, modify, or remove user accounts.

When configuring GlobalProtect, the default configuration is to tunnel all remote access VPN user traffic through the US Signal firewall. This not only includes network traffic destined to private networks that sit behind the Palo firewall, but also user traffic destined to the Internet. While this does provide security benefits as it allows a company to enforce security policies on remote users, it may cause congestion if remote users are utilizing bandwidth-intensive applications such as streaming videos.

To circumvent this bandwidth issue, the Palo Alto supports a Split-Tunnel configuration option. This allows you to specify a list of internal networks to push to connected VPN clients, instead of forcing all traffic over the encrypted VPN tunnel. Traffic destined to the Internet will not be encrypted and will utilize the remote VPN user's local Internet connection. If Split-Tunnel is a desired option, the customer will need to specify which internal networks they want remote users to have access to and provide internal DNS information.