Customer BYO Firewall Appliance Policy

Over the years some customers have asked if they can bring their own firewall appliance ("BYO Firewall Appliance") instead of using the MacStadium provided Cisco ASA firewall appliances. If customer elects to use a BYO Firewall Appliance, customer agrees to comply with the terms and conditions stated in this Customer BYO Firewall Appliance Policy. MacStadium may make changes to this Policy in its reasonable discretion at any time.

Doesn't MacStadium manage the firewall anyway?

No, we currently do not provide any managed firewall services. The shared risk and responsibility model defined by our security & compliance program dictates that MacStadium customers are solely responsible for configuring, managing, and monitoring their BYO Firewall Appliance. Once we initially provision such appliance with its base configuration and turn it over to the customer, we do not maintain control of credentialed access to their environment or their proprietary data. If a customer needs any level of support, we can provide remote hands services or open a TAC case to engage directly with Cisco support. If a MacStadium customer requires managed firewall services, such may need to engage with a third party managed services providers as MacStadium does not offer this type of service. Shared risk responsibility model ("SRM") links: Private Cloud SRM and Orka® SRM

Will MacStadium allow a customer to bring their own firewall appliance?

This unfortunately is not an option that we recommend nor can we guarantee any level of support or SLA uptime. MacStadium is currently unable to provide mission critical production support for any other vendor firewall solutions outside of Cisco ASA. The firewall appliance acts as the gateway for all internal and external network traffic and is critical to maintaining security and connectivity to your environment. If the firewall cannot pass traffic then the environment may be unreachable. Without implementing the proper tools, training, and processes, we are simply cannot ensure any guarantees of MacStadium's Service Level Agreement ("SLA") including but not limited to uptime or availability for any vendor firewall solutions outside of Cisco ASA

What if the customer cannot support Cisco ASA for similar reasons?

We have a small handful of customers who cannot use MacStadium services with the provided Cisco ASA firewall appliance due to their internal policies or procedures. If a customer has extensive 24x7 internal or vendor provided support for their BYO Firewall Appliance, and is comfortable using a remote console session for emergency access, the use of a BYO Firewall Appliance may be approved on a one-off, case-by-case basis, as long as the customer agrees to and adheres by the terms & conditions stated herein.

If a customer chooses to provide their own firewall, what contractual conditions would apply?

If a customer elects to use a BYO Firewall Appliance, MacStadium reserves the right to deny any BYO Firewall Appliance for any reason to be connected to the MacStadium network at any time.

As a note, customer is solely responsible for evaluating all security risks associated with their BYO Firewall Appliance. MacStadium a) provides no guarantees as to the level of security provided by the Customer's BYO Firewall Appliance or the configuration implemented on it; b) does not assume any liability whatsoever for any security breach, degradation in performance, or data loss that may occur as a direct or indirect result of any Remote Hands provided by MacStadium; c) has no obligation to proceed with Remote Hands requested unless and until the parties have agreed by an electronic support ticket; and d) **will not be obligated to uphold any protections or warranties stated in the SLA or be in breach of the SLA due to a misconfiguration or failure of customer's BYO Firewall Appliance**.

Are there any limitations on what BYO Firewall Appliances a customer can use?

The customer may use any BYO Firewall Appliance that meets their functional requirements within the limitations listed below, however, it must be a standard 19" rack-mountable device with AC power and conform to MacStadium's cold isle containment. Additionally, customer shall not use firewall virtual appliances for their MacStadium environment under any circumstances.

- Up to qty 2 1U-2U 19" standard rack mount firewalls per customer environment
- Optional customer provided OoB console server must be 1U.
- Must comply with cold isle / hot isle containment.
- Firewall Must support Multi Mode fiber connectivity.
- Firewall must support 1G or 10G connectivity. (25G with approval)

What will MacStadium charge for colocation of a customer firewall?

The monthly charge will be $150.00 per one (1) rack unit. This includes rack space, power, cooling, network connectivity, and a /29 public IP address block. Additional public IP address space may be sold separatel

Will MacStadium monitor my firewall?

By default, we will only monitor the customer's firewall by ICMP response for basic up down status. For $10.00 per month we can add full LogicMonitor monitoring of the BYO Firewall Appliance if the customer is able to provide the proper access.

How will MacStadium facilitate support?

In the event that a customer requests basic remote hands screen share console access support ("Remote Hands"), a data center technician can be dispatched to power cycle the device or to connect a console cable and provide screen share remote access to the customers support team. Remote Hands may also include providing on request console access, on/off powering of customer's BYO Firewall Appliance, and visual inspection. MacStadium will not provide any configuration support for customer's BYO Firewall Appliance aside from providing information regarding how the customer must configure such appliance to interact with MacStadium's network. Such information may include IP addressing, MacStadium side interface configuration, and VLANs / trunking information.

- Non-emergency console access must be arranged within three (3) business days of the engagement.
- Emergency console access is subject to availability with no guaranteed response SLA all actions will be best effort.

As a note, customers are required to provide their own hardware, software support contracts, and any console server or console cable(s) needed for facilitating Remote Hands. MacStadium may only provide provisions for hardware firewalls.

Will MacStadium allow permanent out of band management capability?

Yes - MacStadium can facilitate with hardware provided by the customer

- Customer can provide a 1U console server
- Console server must follow cold isle/hot isle restrictions and will be changed at the same per 1U cost as the firewall.
- Console server can be provided connectivity either by customer provided cellular based on cell strength or 1G/10G connectivity to switch on same Outside subnet as the firewall.

Will MacStadium need credentialed access?

No credentialed access is needed - console on demand. Customer must provide VPN access to support the infrastructure behind the firewall on demand or by default and a console kit, cataloged by MacStadium.

Where should the BYO Firewall Appliance be shipped?

Customers should be instructed to ship their BYO Firewall Appliance directly to the appropriate data center to the attention of the local site manager. This information will be provided via the service provisioning ticket.

How should the firewall be configured?
The BYO Firewall Appliance is solely the customer's responsibility with regards to configuration and any disaster recovery. The customer should configure and test the firewall before it is shipped to MacStadium. MacStadium will provide the customer with an IP plan and configuration cut sheet through our ticketing system.

- Provide a cut sheet with the IP plan, this will also need to include details about how the IPs are presented.
- Connectivity will be an L3 SVI with Outside subnet GW.
- Static routing only for provided publics to FW IP in outside subnet.
- No support for L3 dynamic routing.
- Only basic IP connectivity.
- Dual firewall setups will be connected to diverse service leaf switches.

What happens if a customer needs to coordinate physical access to the firewall by one of their employees or contractors?

Technician access is not currently allowed. Upon the execution of a nondisclosure agreement, escorted data center tours are available to customers for initial security & compliance inspections.