

Security Response Procedures

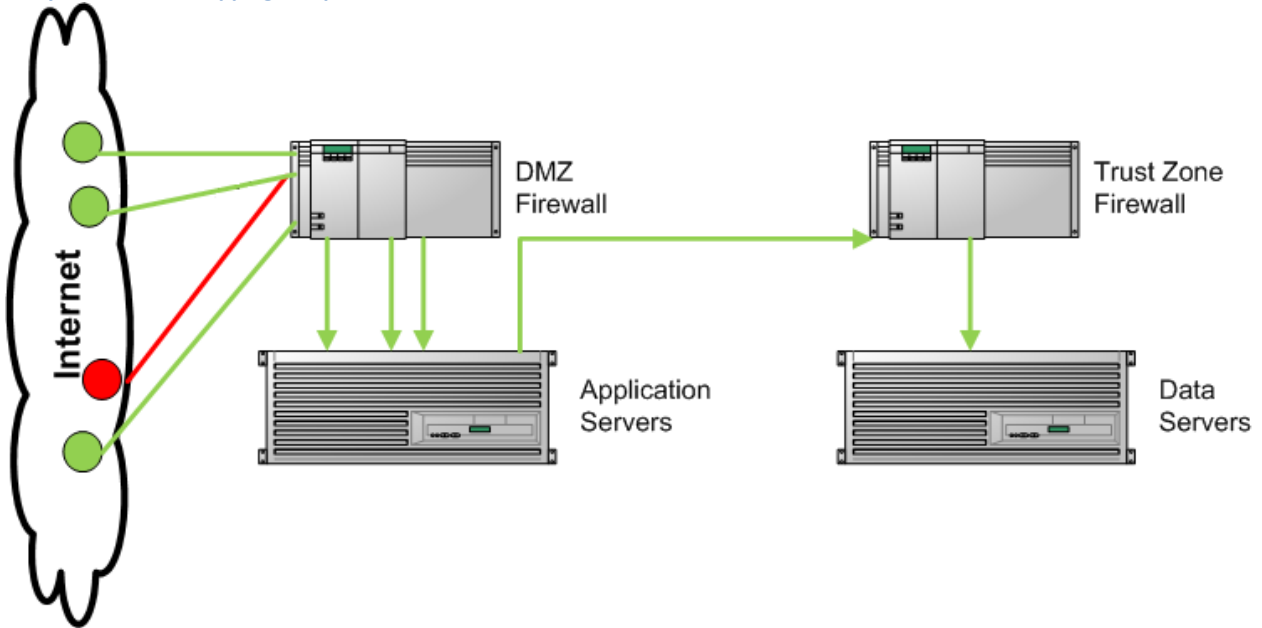
Overview

All Allegiance Application servers are housed within secure data centers. The security and intrusion protection of Allegiance hardware is monitored by specially-trained personnel 24x7x365. Responsibility for guaranteeing appropriate security for data, systems, and networks is assigned to the Allegiance Security Officer. The CTO is currently assigned to this role. The Security Officer is responsible for designing, implementing, and maintaining security compliance. Ongoing review of security requirements may require periodic change or additions to the existing policy. It is the responsibility of the Security Officer to advise management of these changes, and to establish procedures to support the implementation and maintenance of the security policy. Periodically Allegiance reviews its existing policies, and holds an annual meeting with its staff to review current and new procedures.

There are perimeter devices used at the data center for defending Internet accessible systems. This includes managed Firewalls that utilize both a De-Militarized Zone (DMZ) and Trust Zone configuration to protect Allegiance Web servers and access to its Data servers, as well as an Intrusion Prevention System (IPS). Every managed Firewall includes an IPS to monitor activity and to alert of anything suspicious. The firewall is capable of monitoring, logging, and managing spam, spyware, intrusion prevention, and URL filtering.

When an attack is detected by the IPS it can drop the offending packets while still allowing all other traffic to pass. The intrusion detection system can detect many types of malicious network traffic including attacks against vulnerable services, data driven attacks on applications, host-based attacks, unauthorized logins, and malware. Detection can generate security events. The events can be monitored by a console, and result in an automated notification alert. A central engine records database events logged by the detection system, which can be used to generate alerts and automated actions.

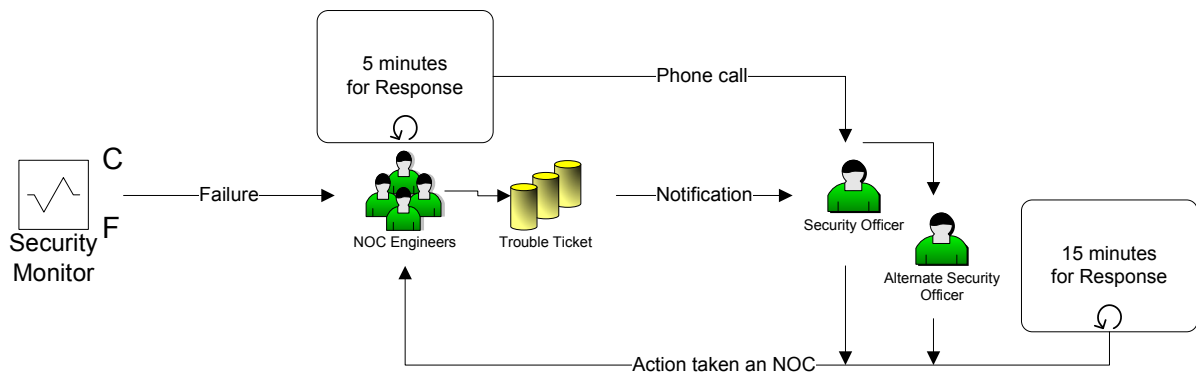
IPS system shown dropping bad packets



Security Incident Management

In the event a security issue has been identified, either through manual or via an IPS event, an alert will be generated. This will result in an incident logged into the trouble ticket system, and notification made to the Security Officer and on-duty Network Operations Center (NOC) staff member. This invokes an email to all parties associated with the incident type. If no response is received within 5 minutes, the NOC staff will initiate a phone call to the primary Security Officer and alternate Security Officer (VP Technology) if the primary Security Office does not respond.

Tickets are investigated by an internal NOC member, and recommendation appended to the ticket. Security Officer is given the option to proceed with the recommendation or provide an alternative recommendation. If a response is not received by a Security Officer or an alternate Security Officer within 15 minutes, the incident is escalated to a NOC staff supervisor to take immediate action. The result of those actions are recorded in the ticket.



Additional Access Procedures

In addition to security events, other monitoring is invoked to ensure servers are accessible continuously throughout the day. Custom monitors are defined to call Allegiance Application web pages, and to analyze page load times. In the event of a page load error or load time threshold condition is not met, an e-mail alert is sent to the Allegiance Technology group and NOC Engineers. The Allegiance Technology group is the first line response team. The team will validate and provide immediate action or direction to address the issue. If the issue is not resolved within 15 minutes, a trouble ticket is logged and assigned to a NOC engineer. NOC engineers will then work with an Allegiance Technology engineer to ascertain and address the issue. If an Allegiance Technology engineer is not available, NOC engineers have been trained to diagnose and fix the failure when possible.

