# Internet Hosting & DMZ Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of this standard is to define the configuration to be met by all servers owned or managed by Alight that are located outside of the firewalls. The standards are designed to minimize the exposure to Alight from damages that may result from malicious activities from both internal and external entities. Internet facing devices located outside the Alight firewalls are considered part of the DMZ.

The standard outlines two goals for the deployment of systems in untrusted Alight controlled environments. The first goal of this standard is to provide an approach to developing an environment designed to appropriately expose web applications to the Internet while protecting the internal network, application data and other applications from exposure. As the word 'appropriately' can be interpreted in many ways, this document's purpose is to define the methodology and architecture of the DMZ design.

The second goal is that this infrastructure is designed for multiple tenant operations and lifecycle support.

* Multiple Tenant Support: Each DMZ segment can house multiple applications, and, if desired, a VLan can be assigned within each DMZ for the express purpose of housing a single application, or a class of applications. Examples of this paradigm would be a VLan within the Web DMZ to support all non-PII bearing applications, and another VLan to support all PII bearing applications.
* Lifecycle Support: Each lifecycle (Production, Prod-Test, or QC) environment must be separated by VLans.

## Standard Statements

### General

* 1. Deployment of new solutions must be approved by Global Security Services (GSS) prior to deployment in an Internet facing role.
  2. Operating System configurations must be performed in accordance with the Alight hardening standards and / or industry regarded best practices.
  3. Public servers (WEB, FTP, DNS, proxy, mail server, etc.) must be placed in DMZ.
  4. Remote administration must be performed over secure channels.
  5. A risk acceptance process must be established to permit access to blocked websites for legitimate business purposes.
  6. With the exception of centrally-managed security devices, no other machine image or individual operating system must have network connections to more than one security zone; this includes systems that share a common backplane but not a common operating system image (e.g., VMware guest instances or individual domains on a multi-domain Sun Enterprise 10K or 15K system); systems that share a common backplane but not a common operating system image may have multiple connections into the same security zone.
  7. Implement logical and functional separation on server platforms (for example, Web Servers, Database Servers, and Domain Name Servers).
  8. Implementations must have design considerations to defend against Distributed Denial of Service (DDOS) attacks.

### Logical Design

* 1. The typical traffic flow of DMZ should be as follows:
     1. Internet --> Choke Router --> Reverse Proxy/Load Blanker --> Firewall --> Web DMZ --> Firewall --> App DMZ --> Firewall --> DB DMZ (or Shared DMZ Farm)

### Logical design considerations:

* 1. Choke Router
     1. A choke router must be used to screen the environment from the Internet. It must be used to cut down the number of services visible to the Internet.
     2. The choke router must not have administrative interfaces revealed to the broad Internet.
  2. Reverse Proxy
     1. The reverse proxy may be used to terminate SSL sessions and pass unencrypted web data to the web server for processing. The determination is defined by the data classification type which is defined in the Data Security Classification Standard.
     2. The reverse proxy must be addressed with public IP addresses.
  3. Web DMZ
     1. The Web DMZ houses the first exposed architecture of the application to the Internet. This layer commonly supports web services.
     2. The web DMZ must be addressed with private IP addresses.
     3. The Web DMZ must be allowed to initiate communications with the App DMZ on an IP to IP via port basis.
     4. The Web DMZ must not be allowed to initiate communications with the DB DMZ.
     5. The Web DMZ must not be allowed to initiate communications with the internal network.
     6. The Web DMZ must not be allowed to initiate communications with the Internet.
     7. Systems in the Web DMZ must not persistently store PII/PHI.
  4. Application (“App”) DMZ
     1. The App DMZ houses many of the different processes within an application architecture, but is not Internet facing and does not persistently store PII/PHI.
     2. In general, the App DMZ must not be allowed to initiate communications with the Internet. The exception to this is when applications require external web services content to be rendered within the application. An example of this could be participating plan doctors within a health benefits portal. When the App DMZ needs to connect to the Internet for web services, the following requirements must be met:
        1. The connection must be constrained to a source port (Application server(s)), destination port for each web services call.
        2. The connection must be facilitated by a Proxying technology.
     3. The App DMZ must not be allowed to initiate communications with the internal network.
     4. The App DMZ must receive connections from the Web DMZ and must forward requests for information to the DB DMZ.
  5. Database (“DB”) DMZ
     1. The DB DMZ is the only layer of the DMZ infrastructure that is allowed to store PII/PHI.
     2. The DB DMZ must not be allowed to initiate communications to the internal network.
     3. The DB DMZ must not be allowed to initiate communications with the Internet.
  6. Firewall
     1. Each firewall must explicitly allow specific services from a defined source to a specific destination on specific ports.
     2. Firewall administrative / management interfaces may not be externally routable or accessible from any other network segment other than the internal network.

### Infrastructure Management

* 1. Firewall and Network Management
     1. Processes must be established and followed that are designed to ensure that all firewalls and other network security enforcement devices, including but not limited to, choke routers, reverse proxies, and switches are managed using industry-standard security and change management practices.
     2. All firewalls and other network security enforcement devices, including but not limited to choke routers, reverse proxies, and switches are managed using encrypted communication channels.
     3. Firewall management must also require two-factor authentication which includes a non-reusable password.
     4. Firewalls must be managed by an Alight IT Service organization or an outsourced IT Service delivery partner, and not by business unit IT personnel, to ensure proper separation of duties.
     5. Firewall rule bases must be audited annually at a minimum.
  2. Vendor Access
     1. Third parties (vendors) may be used to support systems located in the DMZ infrastructure.
     2. Vendors must be granted access to a restricted scope of servers (per IP assignment) as appropriate with their duties. Call alter access is recommended using password vault technologies for all vendor granted access to prevent unauthorized access.
     3. Each system that is serviced by a vendor must have technology installed that prevents the user from leaving that system (Appease for Windows, None for Solaris/Linux).
     4. On-site vendors (contractors) must use a corporate imaged system, with all appropriate controls, commensurate with the supported business requirements (i.e., DLP, AV, etc.).
     5. Off-site vendors must connect to the network using an approved and policy supported method (i.e., Citrix) and must not be allowed to map local drives to the remote server.

### Physical Design

* 1. While the logical design considerations are important, there are specific physical implementation architecture decisions that must be defined.
  2. Firewalls
     1. The logical design indicates that there must be a firewall between each layer of the infrastructure.
     2. The physical design demands that one physical firewall must support the 'dirty' environment.
     3. The physical design demands that one physical firewall must support the 'clean' environment.
  3. Network Switches
     1. The logical design indicates that there must be individual network(s) within each layer of the infrastructure.
     2. An individual or set of VLans must be used to support each security zone/DMZ layer.
     3. All traffic destined for an adjacent DMZ must be forwarded to the appropriate firewall for access control list (ACL) evaluation.
     4. The physical design demands that physical network switching platforms must only support one classification of environment (e.g. ‘clean’ or ‘dirty’). See Appendix I for clarification.
  4. Network Device Connection
     1. No system must have connections with more than one security zone, with the only exceptions being:
        1. Firewalls: Used to negotiate security between security zones.
        2. Carrier Grade Network Switches: Used to support DMZ VLans and support connections with those VLans to firewalls.
     2. A single blade enclosure must only have physical network connections into one DMZ. A blade enclosure is not allowed to connect to multiple DMZ segments.
     3. A single VMware Chassis must only have physical network connections into one DMZ. A VMware Chassis is not allowed to connect to multiple DMZ segments.
  5. Storage
     1. Storage Area Networking (SAN) Definitions:
        1. SAN disk assignments are defined in two different methods:
           1. Per Host
           2. Clusters
        2. Each host must have a single LUN assigned and must be connected to the storage fabric via redundant paths. The only exception to this rule is if a cluster is required.
     2. Network Attached Storage (NAS) Definitions:
        1. NAS must be defined as a CIFS drive or NFS drive.
        2. A NAS resource must be defined into different logical units by a vFiler.
        3. A single NAS resource can be used by multiple servers.
        4. A single NAS resource can only be used within a single DMZ or security zone.
        5. All NAS resources must require the use of authentication credentials for access.
        6. Each application within the DMZ infrastructure must utilize its own vFiler.

### Data Classification and Usage

* 1. Production data must only be used in Production lifecycles, and when required by the client in Prod-Test/QC.
  2. Data migration from production to any other environment requires for data to be scrubbed of HBI and MBI data and requires the authorization from Global Security Services as stated in the Information Security and Privacy Policy.

### Application/System Entry Processes

* 1. Appropriate change control must be required in Internet facing zones to manage changes.
  2. All servers must be scanned and clear of system vulnerabilities before entry into the DMZ infrastructure.
  3. All applications before being cleared for production and advertised to the Internet must pass the following processes:
     1. An infrastructure review which validates that the design passes all applicable policies and standards with regards to configuration and placement of components in each DMZ.
     2. An application level audit which validates that appropriate application layer vulnerabilities have been reviewed and mitigated.
     3. The CISO must assist the project team with contacting the appropriate resources for the project.
  4. Any exceptions to policy or security defects discovered by the Vulnerability Scan, Infrastructure Review or Application Audit that are not remediated before the go-live date must be signed off by the business segment CIO and the Regional/Global CISO before the system is granted production status.

### Third Party Managed Devices

* 1. All devices managed by third parties must adhere to the Supplier Policy and Standard as well as all related Alight Policies and Standards.
  2. The responsibility for the security of equipment deployed / managed by third parties must be stipulated in the contract with the third parties as follows:
     1. Security contacts and escalation procedures must be documented and revised on a regular basis. Minimally this must occur on an annual basis or when there are changes in personnel who are involved in the management of the devices.
     2. Each party's access and privileges must be restricted only to their data environment.
     3. Processes must be defined to facilitate timely forensic investigations in the event of a security incident.

## References and Mandates

* None

## Legal Conflicts

Alight Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard of Alight shall take precedence over the more general provisions contained in Alight Security Policies and Standards.

# Appendix I

### Internet Hosting DMZ Diagram



# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_201.08 Internet Hosting & DMZ Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.6 |
| Owner | Alight Global Security Services | Information Security |
| Author(s) | Alight Global Security Services | Information Security |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 2, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 March | Original | Restructured due to Aon Hewitt merger |
| 1.1 | 2013 June | 2013 Annual Review | Reviewed and validated |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.4 | 2015 November | Update Wording | Added wording for denial of service |
| 1.5 | 2016 June | 2016 Annual Review | Updated name change from IRSS with Global Security Services (GSS) to reflect new organization name; wording change for clarity; updated wording to distinguish server OS |
| 1.6 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |