

<Your Company Name>

DMZ Security Policy

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in <Company Name> located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to <Company Name> from the damage to public image caused by unauthorized use of <Company Name> resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope

<Company Name> networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside <Company Name> corporate Internet firewalls are considered part of the DMZ(s) and are subject to this policy. This includes DMZ(s) in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents.

3.0 Policy

3.1. Ownership and Responsibilities

1. All new DMZ(s) must present a business justification with sign-off at the business unit Vice President level. InfoSec must keep the business justifications on file.
2. Organizations are responsible for assigning managers, point of contact (POC), and back up POC. The owners must maintain up to date POC information with InfoSec [and the corporate enterprise management system, if one exists]. Managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ(s) and establishment of new DMZ must be requested through a <Company Name> Network Support Organization and approved by InfoSec.
4. All ISP connections must be maintained by a <Company Name> Network Support Organization.
5. A Network Support Organization must maintain a firewall device between the DMZ(s) and the Internet.
6. The Network Support Organization and InfoSec reserve the right to interrupt connections if a security concern exists.
7. The DMZ will provide and maintain network devices deployed in the DMZ up to the Network Support Organization point of demarcation.
8. The Network Support Organization must record all DMZ address spaces and current contact information [in the corporate enterprise management system, if one exists].
9. The DMZ Managers are ultimately responsible for their DMZ complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*
11. Individual accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
12. InfoSec will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ networks.
2. DMZ must not be connected to <Company Name>'s corporate internal networks, either directly or via a wireless connection.

3. DMZ should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Manager must maintain a list of who has access to the equipment.
4. Managers are responsible for complying with the following related policies:
 - a. *Password Policy*
 - b. *Wireless Communications Policy*
 - c. **Anti-Virus Policy**
5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ business needs. All firewall filters will be maintained by InfoSec.
6. The firewall device must be the only access point between the DMZ and the rest of <Company Name>'s networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec (including both general configurations and rule sets). InfoSec may require additional security measures as needed.
8. Traffic from DMZ(s) to the <Company Name> internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ running Internet Services must be configured to the secure host installation and configuration standards. [Add url link to site where your internal configuration standards are kept].
11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
13. Services and applications not serving business requirements must be disabled.
14. <Company Name> Confidential information is prohibited on equipment where non-<Company Name> personnel have physical access in accordance with the *Information Sensitivity Classification Policy*
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Terms

Access Control List (ACL)

DMZ (de-militarized zone)

Network Support Organization

Least Access Principle

Definitions

Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

Networking that exists outside of <Company Name> primary corporate firewalls, but is still under <Company Name> administrative control.

Any InfoSec-approved support organization that manages the networking of networks.

Access to services, hosts, and networks is restricted unless otherwise permitted.

Internet Services Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.

Network Support Organization Point of Demarcation The point at which the networking responsibility transfers from a Network Support Organization to the DMZ. Usually a router or firewall.

Manager The individual responsible for all network activities and personnel.

Firewall A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.

6.0 Revision History

© SANS Institute 2006, All Rights Reserved