Moving Public Services into a DMZ

Version 7/11/2003

Background

- The “Interim Authority to Operate” status of the NWIS system expires Sept. 30, 2003. Funds will be taken away from the NWIS Program Office if it does not pass the Office of Management and Budget Circular A-130 Certification & Accreditation (C&A) process by September 30. The C&A package is due at DOI August 29th.
- For NWIS to pass the C&A process, NWIS servers cannot be in the same local area network (LAN) subnet as servers providing public services.
- To accomplish this separation, all public services at an NWIS site will have to be either moved to the Bureau http and FTP servers (e.g. NatWeb), or placed in a DMZ. A DMZ is a logically separate network from the private network that provides containment in the event that the public server is compromised.
- A DMZ will consist of an Internet-accessible subnet separated from the “private” subnet and protected by policies limiting public access to well defined services.
- Access will be restricted into, and OUT of, the DMZ. Firewall rulesets will be constructed based on a default "deny all" with access only to specific services/ports and source/destination host IP addressing. Firewalls for the public DMZ will not to have any generic trusted "allow all services” relationship to servers or services on the private internal USGS networks.
- At NWIS locations where public services are required locally, a DMZ will be configured by the Bureau Information Technology Security Operations Team (ITSOT) and Geonet Team on the site’s Cisco router. Until further notice, a DMZ configured on a router will be considered a temporary DMZ. Temporary DMZs are allowed only for one year.
- Permanent DMZs will be installed, in the future, at limited sites following GIO approval of their business needs for a local DMZ. The process for requesting approval has not yet been determined.
- Before the year is up, sites that have a temporary DMZ will either move their public services (FTP, http) to the Bureau's consolidated http system (NatWeb) and consolidated FTP system OR submit their business case to request a permanent DMZ. Most sites are expected to migrate all public services to the Bureau’s consolidated systems.
- By August 29, 2003, all servers providing public services must be moved into a local temporary DMZ
- All DMZs will undergo unannounced security scans several times per year or whenever major changes are made to servers or firewalls. DMZ firewalls will have a defined rule to allow access from a central vulnerability-scanner host.

Preparing to move servers to a DMZ

- From the router firewall configurations the publicly accessible servers can be determined by finding the “permit tcp/udp any” syntax. A spreadsheet of all public servers per site will be sent to the lead SA at each NWIS site. The servers on this list must be moved into the DMZ. If you rather restrict the service to specific IPs or remove it from the firewall config, please email your request to GS-W Help Firewall.
- If you followed Sun_TACs public webserver recommendations, your NWISWeb server should be ready to be moved to a DMZ.
- Servers that are moved into a DMZ need to meet many requirements defined in the DOI Perimeter Security Standards many of which involve detailed planning and will be brought to you attention at a later date, but to make the initial migration the servers should have the following:
    1. Logging and reporting (who’s using the servers)
    2. Windows servers must use antivirus software.

3. Password controls
4. Patches – applied in a timely manner; critical security patches within 48 hours
5. Change Management Review- a process to document and decide how, when, and why changes will be made to a system. Symantec's ESM software will be part of this process and eventually be installed on DMZ hosts. To maintain consistency WRD will provide further guidance regarding this process.
6. Copies of the data on the servers in the DMZ must be available so that the servers can be recovered.
7. COOP (disaster recovery and contingency plan)
8. Hosts residing in the DMZ should use host-based intrusion detection systems. At a minimum, they should use a file change detection system, such as Tripwire or sum_files to detect changes of critical operating system files.
9. Standard Operating Procedures (as defined by advisory teams like NT_TAC and SUN_TAC).

- All applications and software packages not used on USGS public systems must be disabled. For example, telnet should be disabled. All files not permitted on USGS public systems must be removed.
- Servers that are moved to a DMZ should **not**:
    1. Authenticate to an NIS server or Windows Domain in any private subnet.
    2. NFS-mount file systems in other than a READ ONLY configuration.
    3. Have Windows or Samba file shares to computers that reside in your private subnet
    4. Print or have print shares to a printer in your private subnet
- The only traffic that will be allowed to pass from a DMZ into your LAN is access from a web application to a backend database (Oracle, ArcIMS, etc.)
- Synchronization (rsynch) is allowed when it is initiated from the LAN (in a push mode).
- Not allowing servers in the DMZ to authenticate into the private LAN raises the problem of having to maintain a separate user database on the servers you moved to the DMZ. Three possible ways to allow users to edit data files that are published from the DMZ are:
    1. Rsynch. Rsynch runs on Linux, Solaris and Windows – Rsynch can be set up to replicate (push) changes in a directory to the servers in the DMZ. Since the server initiating the rsynch remains within your LAN, users will be able to authenticate and write to this area as they currently do. Using this approach will make the transition to the Bureau consolidated FTP system much easier because you will just have to point rsynch to the central server.
       Sun_TAC instructions: http://wwwqvarsa.er.usgs.gov/unix/solaris/rsync.html
       How to rsynch: http://www.physics.queensu.ca/Computing/Docs/HOWTOs/rsync/
       Windows: http://optics.ph.unimelb.edu.au/help/rsync/rsync_user.html
       How to Tunnel rsynch through ssh: http://killyridols.net/rsyncssh.shtml

    2. Limit accounts. Assign the task of moving files to the DMZ to a few individuals instead of allowing all users. You need only to create and maintain a few local user accounts on the servers in the DMZ.
    3. RO NFS mount. The directory that users currently have access to edit (e.g. /var/ftp/pub) can be mounted as a READ-ONLY partition on the public server(s) in the DMZ. Allowing NFS traffic between the DMZ and your internal network raises a "medium" threat, therefore, tight controls must be kept to ensure that it is configured correctly. The following document from the BITSM outlines the risks involved and how to request a waiver to use NFS in this manner: http://wwwnwis.er.usgs.gov/SECURITY/NFS.pdf

Other issues to consider:

- The IP address of your local public server(s) will change. All servers in a DMZ will have a new IP address range nationwide. Each site will be assigned a minimum block of 14 IPs in the DMZ subnet (16 when counting subnet and broadcast addresses). **USGS DMZ address space is 137.227.224.0/19**

CR DMZs - 137.227.224.0 - 137.227.231.255 - (137.227.224.0/21)
WR DMZs - 137.227.232.0 - 137.227.239.255 - (137.227.232.0/21)
ER DMZs - 137.227.240.0 - 137.227.247.255 - (137.227.240.0/21)

- A switch or hub will be needed if connecting more than one server to the router's "DMZ port/interface." ITSOT is ordering a 24 port switch for every office.
- If you have local Lotus Domino servers, they will be moved into your local DMZ. The Lotus group will be coordinating this move.
- FastEthernet (100BaseT) cannot be expected between the public and private subnets connected to the router. The router interface supports only 10Mbit Ethernet speeds.
- If you are currently offering public services and internal services from one server, you will need additional equipment to split these functions to separate servers. For example, if your FTP server is also your NWIS server you will need to remove the ftp functionality from the NWIS server. This service could possibly be moved to your NWISWeb server which will also be in the DMZ.
- Direct access to NWIS servers will be granted to cooperators provided that these conditions are met.

  1. Prior to granting access a Memorandum of Understanding (MOU) is signed between the local NWIS Database owner (usually the District Chief) and equivalent management at the cooperative agency. See this URL for WRD policy on cooperator access:

     http://oregon.usgs.gov/uo/tac/tr93.2d.pdf

  2. Each individual at the cooperative agency is granted a personal userid.

  3. Access into your private network is allowed through the firewall using secure shell (ssh) by specific IP address (source and destination IP addresses must be defined).

  4. TCP/IP wrappers are configured on the NWIS server and access is granted for secure shell by specific IP address.

  Additionally, it is strongly recommended that cooperators access the NWIS server using a restricted shell. See this URL for details:
  http://wwwdcascr.wr.usgs.gov/~dkyancey/coop.html

Overview of Bureau Consolidated Systems
Moving local public services to the Bureau's consolidated http system (NatWeb) and consolidated FTP system is still necessary because DOI is expecting the USGS to reduce the number of publicly accessible Web and FTP servers. Migrating to the consolidated systems will relieve you from responsibilities like preparing business cases, getting DOI waivers and adhering to DOI security standards.

Proposed Consolidated FTP System: The Bureau's centralized FTP server will use rsynch to synchronize with a designated directory (depot) in your private LAN. The rsynch process will be initiated in a push fashion from the server that houses this depot. FTP access will be blocked at your local firewall. Users will be able to move files to and from your local (now internal) FTP server as they always did. If your site usually allows users to write to the FTP directory via an NFS mount you will be able to completely disable the FTP services. The Bureau IT Security Operations Team (ITSOT) is working—in parallel to the creation of DMZs—on deploying public anonymous FTP READ and WRITE services before Sept 30. This approaching deadline does not

allow enough time for sites to migrate to the consolidated systems but will show DOI progress in our efforts to meet their mandate to consolidate public services. Sites will be expected to maintain their local "depots" organized and to perform routine cleanups. Reasonable quotas might be implemented in the future if needed.

Consolidated Web System: The NatWeb Team provides on-line information about migrating to NatWeb. NWIS-RT is also now available.

Please answer these questions and send responses to your Regional Computer Specialist (NR=ealv, SR=jimbett, CR=wsmcewen, WR=tejmoore)

1. Can you anticipate any problems or reasons why your site would not be able to migrate to the consolidated FTP or Web systems? In other words, does your site have special needs which you feel are not being addressed?
2. If you have public IIS web servers, explain why your needs can only be met by IIS and not Apache.
3. If your site's only public service is http and you intend to move your public http service to NatWeb by August 30th, then your site probably does not require a DMZ. Do you need a DMZ? (Y/N)