



Network Infrastructure Security Good Practice Guide

August 2009



contents

1	Introduction to Good Practice Guides	3
2	Network Infrastructure Security Overview	3
2.1	Understanding 'Good' and 'Better' Practice	3
2.2	Key Requirements of Network Infrastructure Security	4
3	Internal Network Architecture	4
3.1	Internal LAN requirements	4
3.2	Security of Network Services	4
3.3	Storage of sensitive information on Networked Systems	5
3.4	Network Connection Control	5
3.5	Administrative Services	5
3.6	Networks supporting Test and Development environments	6
3.7	Documentation of network configuration and architecture	6
3.8	Visitor access	6
3.9	Access to internal applications	6
3.10	Virtualized Environments	6
4	External Connection Guidelines	7
4.1	Third Party Access to Internal Networks	7
4.2	User Authentication for External Connections	7
4.3	Segregation of Internet Connections	7
4.4	Wireless Connections	10
4.5	Modem Connection	11
5	Network Device Configuration Guidelines	12
5.1	Firewalls	12
5.2	Routers	13
5.3	Bandwidth Accelerator / Prioritisation Devices	13
5.4	Modem Concentrator Devices	14
5.5	Content Filters	14
5.6	LAN Switches	15
5.7	Network Intrusion Detection/Intrusion Prevention Systems	16
5.8	Antivirus	16
5.9	Wireless Access Points	16
5.10	VPN Devices	17
5.11	Web Proxy Servers	17
5.12	VoIP Gateway	18
6	Appendix A: Definitions	19
7	Appendix B: Checklists	21
7.1	Good Practice Checklist	21
7.2	Better Practice Checklist	22
8	Document Control	23

figures

Figure 1: Internet Connection Design Pattern (single firewall)	8
Figure 2: Internet Connection Design Pattern for Application Hosting	9
Figure 3: Wireless Connection Design Pattern	10
Figure 4: Modem Connection Design Pattern	11
Figure 5: VoIP Connection Design Pattern	18

1 INTRODUCTION TO GOOD PRACTICE GUIDES

This document is a good practice guide concerning ICT network infrastructure security within the various international agricultural research centers that are supported by the Consultative Group for International Agricultural Research (CGIAR). This guide forms part of the CGIAR-wide baseline ICT Security and Acceptable Use good practice set. The target audience for the good practice guides are all centers affiliated with CGIAR, and in particular, the IT teams within each center.

The good practice set does not contain mandatory requirements that centers are required to implement. Instead, it outlines a number of good practices with respect to enterprise ICT security and acceptable use. The prudence of implementing specific good practices identified in this guide will depend on the risk profile associated with the ICT environment in each center. A set of checklists is provided at the end of this guide to assist with the process of determining those good practices which will be relevant depending on the risk profile of each center.

The initial ICT Security and Acceptable Use good practice set has been prepared in consultation with the CGIAR center IT community under a process jointly managed by the CGIAR ICTKM Program and the CGIAR Internal Auditing Unit (IAU). This guide draws on the results of work undertaken in the CGIAR Enterprise Security and Business Continuity Project; additional inputs from the IT community, internal auditors, and from SIFT Pty Ltd, an information security and risk management services firm which assisted in the preparation of these guides. The ICTKM and IAU units will coordinate future updates in consultation with the CGIAR center IT community.

2 NETWORK INFRASTRUCTURE SECURITY OVERVIEW

Engaging in good practices with respect to network infrastructure is an important component of ensuring that potential threats to the overall ICT security posture of CGIAR centers are managed effectively. This is particularly the case given the shared CGIAR electronic network, which has created an inter-dependency among centers with respect to network security. Specific risks that may eventuate if network infrastructure security is not managed properly include:

- **Loss of data confidentiality:** Data transmitted over a network is at risk of eavesdropping by an unauthorised party. Additionally, weak controls over access to the network may result in data stored on servers or workstations being subject to unauthorised access.
- **Loss of data integrity:** Data may be modified in transit between network nodes, deliberately or otherwise. This may result in the receiving system processing incorrect or malicious data with direct impact upon a CGIAR center.
- **Denial of Service:** A networked system relies upon the continued functionality of all network links that connect its component nodes. The disconnection or slowdown of a network link may prevent a system from providing the necessary services for CGIAR centers to operate.
- **System compromise:** Networked systems within CGIAR centers - including routers, DNS servers, modems and other connectivity devices - are at risk of compromise and their resources being used for such illegitimate purposes as denial-of-service (DoS) attacks, bandwidth theft or aiding in further system compromise.

2.1 Understanding ‘Good’ and ‘Better’ Practice

Although this document predominantly contains good practices for network infrastructure security, these are also supplemented by a number of guidelines which provide for a higher level of security, considered “better” or “best” practice. The difference between good and better practice in the context of CGIAR centers is defined below:

- **Good Practice** - An appropriate set of security controls for most CGIAR centers and network environments. Focus is applied to the use of technologies which are already likely to be in place, and an attempt is made to minimise the complexity of the solutions and the management overhead of the environment.
- **Better Practice** - A higher standard, to provide further guidance to CGIAR centers who have identified their systems or networks as being at an increased risk of attack, where more sensitive information and systems are housed, and where additional resources are available.

2.2 Key Requirements of Network Infrastructure Security

The good and better practices listed in this guide are designed to cater to the following overarching network infrastructure security principles:

1. Network devices should be configured securely and accessed in a secure fashion
2. Secure protocols should be used for network communications
3. Internal and external facing networks should be appropriately segregated through the use of demilitarized zones (DMZs) and control devices such as securely configured firewalls or router Access Control Lists
4. Remote access to internal networks should be managed securely
5. Internal networks should be configured to prevent or detect attempted unauthorized connections and the flow of suspicious traffic

Given that many of the good and better practice guidelines listed in this document are technical in nature, CGIAR centers can, where necessary, engage the services of external service providers or other 3rd parties in order to facilitate their implementation.

3 INTERNAL NETWORK ARCHITECTURE

3.1 Internal LAN requirements

The architecture of internal networks in CGIAR centers should ideally enforce the separation of different types of CGIAR networked systems (such as workstations and servers) into distinct VLANs, and routing should be enabled to allow for communication between VLANs and the creation and management of isolated security domains.

3.2 Security of Network Services

It is recommended that there is a clear understanding of the security characteristics and implications of network services (especially external network services) before these services are enabled for use on CGIAR networks. Relevant security characteristics and implications to consider include:

- The direction of the connection to the network service. Connections to or from external networks such as the Internet to internal CGIAR center networks should involve the use of secure network services.
- Whether the data flowing over the connection to the network service is sensitive in nature (for example, financial or research data). If so, such data should be encrypted to prevent interception by third parties – for example, through the use of secure network services such as SSH for terminal sessions and SSL for data exchanged with websites

All enabled network services (inbound and outbound) should support an approved and documented CGIAR center business purpose.

3.3 Storage of sensitive information on Networked Systems

It is recommended that CGIAR centers maintain a policy which requires that sensitive information (such as financial information and non-public research data) is not stored on systems in CGIAR centers that are connected to or directly accessible from external hostile networks (such as the Internet). Similarly, database and other servers that store sensitive information should not be directly accessible from the Internet. The use of network security zones as explained in section 3.1 will assist in implementing this guideline.

3.4 Network Connection Control

It is recommended that CGIAR centers maintain a policy that, where possible, the connection capabilities of users to CGIAR networks is restricted through techniques such as limiting network access to specified users during certain times of the day or week; allowing only one-way file transfer so that users are not able to upload malicious files to a network; and using VLANs to facilitate separation of network devices and hosts (particularly workstations and servers) so that uniform filtering policies can be applied as necessary to ensure that CGIAR workstations are only able to access network services they require for business purposes. Examples of good filtering policies include:

- An explicit rule is added to ensure that all workstations and servers cannot connect directly to the Internet; connections to the Internet should take place through the use of a proxy server.
- A rule or number of rules is added to ensure that all workstations can connect to the appropriate servers required for proper functionality, such as file, print, application and e-mail servers. If finer-grained access control to resources is required (for example, access to file shares needs to be restricted on a per-user basis) this can be implemented through the use of an Active Directory or similar authentication / authorisation setup.
- A rule is added to ensure that all workstations within a network segment can connect using appropriate network ports to the relevant proxy server serving that segment.
- A rule is added to ensure that all workstations connected to network segments that require authentication can connect to systems hosting authentication services (such as active directory controllers) in order to authenticate users

Systems with open network ports that are deemed unnecessary for business operations should make use of a software firewall installed and running on them. Alternatively, these open ports should be disabled where possible. For more information about appropriate configuration of firewalls, refer to Section 5.1. For more information about configuration of VLANs, refer to Section 5.6.

3.4.1 Network Connection Control – Better Practice

In addition to the above good practice controls, the following better practice control is also recommended:

- IPsec policy filtering should be used to control workstation access to servers

3.5 Administrative Services

It is recommended that the availability of administrative services on CGIAR systems and devices is restricted to authorised internal IP addresses. Authorised internal IP addresses could, for example, include IT managers or system, network and database administrators.

3.6 Networks supporting Test and Development environments

It is recommended that CGIAR centers maintain a policy whereby the environments supporting production, test and development systems are divided into separate logical networks to avoid information leakage and access violations.

Development environments refer to networks supporting systems that are under active development and in which changes occur frequently. Test environments refer to networks supporting systems or which are stable for the purposes of testing. These environments should implement the following, as appropriate:

- Access from development and test systems and environments to production systems or environments should be carefully restricted to the minimum that is necessary. This can be achieved through the use of VLANs or other access control mechanisms such as firewalls.
- Production data should not traverse development and test environments unless absolutely necessary. Where such production data is used in a development or test environment, it should be subject to the same security controls as are present in production.
- Access to development and test networks should be restricted to approved users
- Testing environments may have access to development environment components however this should be restricted to the minimum required to satisfactorily complete testing

3.7 Documentation of network configuration and architecture

It is recommended that the specific network configuration and architecture in place within CGIAR centers is documented by that center. This documentation should include high level network diagrams where appropriate. The documentation should be kept secure and only accessible to authorized staff.

3.8 Visitor access

CGIAR centers may choose to make available dedicated networks for visitors to obtain access to specific resources such as Internet access. It should not be possible to use these physical or logical networks setup for visitor access to access the internal network of CGIAR centers.

A captive portal should be in place on visitor networks that requires visitors to agree to acceptable use terms and conditions as set by the center. Once visitors agree to these terms and conditions, they should only be given access to external networks required for business purposes (this may be restricted to Internet access which is bandwidth and service limited)

3.9 Access to internal applications

It is recommended that CGIAR centers maintain a policy that where an application located within one CGIAR center needs to be accessed by other centers, this should occur through the use of a VPN and should be on a needs-basis only. More information about VPN configuration is provided at section 5.10.

3.10 Virtualized Environments

The implementation of a system as a 'virtualised' environment, does not alter the network security requirements of that system. In particular, where systems would otherwise under this good practice guide require placement into different network segments, this requirement continues to exist in the event that these systems are virtualised. In addition, a physical server should only co-host virtualised systems that belong in the same

network zone (for example, a physical server should not host both a database and a web virtual system since these belong in different network zones).

4 EXTERNAL CONNECTION GUIDELINES

4.1 Third Party Access to Internal Networks

It is recommended that CGIAR centers maintain a policy which requires that in-bound access to CGIAR center internal networks via Internet, VPNs or dial-up access is not granted to third parties unless the IT manager within the center determines that there is a legitimate need for such access. If there is a legitimate need for access, the access should only be granted for the time period required for the 3rd party to accomplish their approved tasks.

4.2 User Authentication for External Connections

It is recommended that CGIAR centers which host applications, services or data that are externally accessible, maintain a policy that access to these via external connections (including for diagnostic or maintenance purposes) should only be permitted if a user has been identified and authenticated as an authorised user. It must not be possible to bypass authentication. Access by the general public to applications intended for anonymous use is an exception to this requirement.

The strength of the user authentication mechanism deployed will depend on the criticality or sensitivity of information assets handled by the network. Appropriate authentication mechanisms include, but are not limited to:

- Hardware tokens
- Cryptographic techniques
- Challenge / response protocols

It is recommended that at minimum, any user requiring a connection into the internal network should be connecting via a VPN using one or more of the following VPN technologies:

- Layer 2 Tunneling Protocol (L2TP)
- IPSec
- SSL utilising a minimum of 128-bit encryption

The IT Manager is responsible for authorising the appropriate level of authentication required, based upon a risk assessment of the internal network being accessed.

4.3 Segregation of Internet Connections

It is recommended that CGIAR centers maintain a policy whereby internet connections are to be segregated from other internal CGIAR center networks via a minimum of one control point (not including the perimeter router/firewall itself). Internet connections should be treated as a hostile network.

4.3.1 Internet Connection – Good Practice

In order to protect CGIAR center Internet connected networks, it is recommended that the following good practice controls are adhered to:

- All incoming and outgoing traffic passes through, and is filtered by a transport layer firewall or equivalent device as it leaves and enters the CGIAR center's network. This device will be referred to as the Internet Firewall
- The Internet Firewall allows only the minimum set of service types required for business purposes to be accessible to and from systems in the Internal Network.
- Any production, development and test / acceptance networks are segregated physically

The following diagram depicts the proposed CGIAR good practice approach to implementing Internet connection architecture at a CGIAR center:

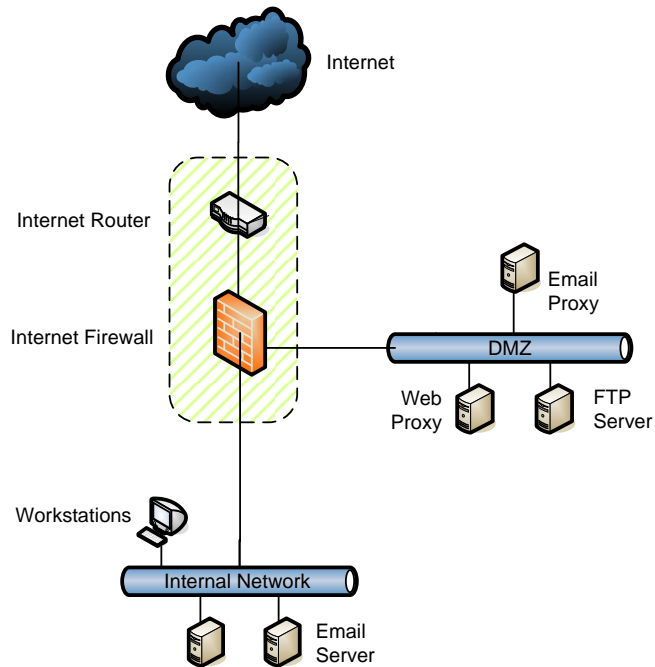


Figure 1: Internet Connection Design Pattern (single firewall)

Note 1: The Internet router and Internet firewall in some scenarios may be combined into a single device as depicted in the diagram. This will vary from country to country depending on the type of Internet service and telecommunication technology used to terminate this service at the business premise. This type of Internet service and the telecommunication technology will dictate if a separate router is required.

Note 2: The email proxy serves a different function to the web proxy in that the former is concerned with transporting emails to and from the email server located in the internal network. Furthermore, this server acts as the client access server for such technologies as Outlook Web Access (OWA) and Remote Procedure Calls (RPC) over https.

In addition to the above good practice controls, these additional good practice controls are recommended if a CGIAR center chooses to host applications accessible externally¹:

- All traffic to and from Internet-facing systems is not able to communicate directly with non-Internet facing systems without traversing and being filtered by an application layer firewall or equivalent device (such as a proxy). This device will be referred to as the Inner Firewall.
- In the event of Internet facing systems being implemented, all Internet-facing systems are logically located in a De-Militarised Zone (Internet DMZ) which is created by the Internet Firewall

¹ This may modify the Design Pattern shown in Figure 1

- The Inner Firewall allows only the minimum set of service types required for business purposes to be accessible to and from systems in the Internet DMZ.
- All systems in the Internet DMZ have anti-virus software installed

The following diagram depicts the proposed CGIAR good practice approach to implementing Internet Connection architecture at a CGIAR center where applications are hosted which are accessible externally:

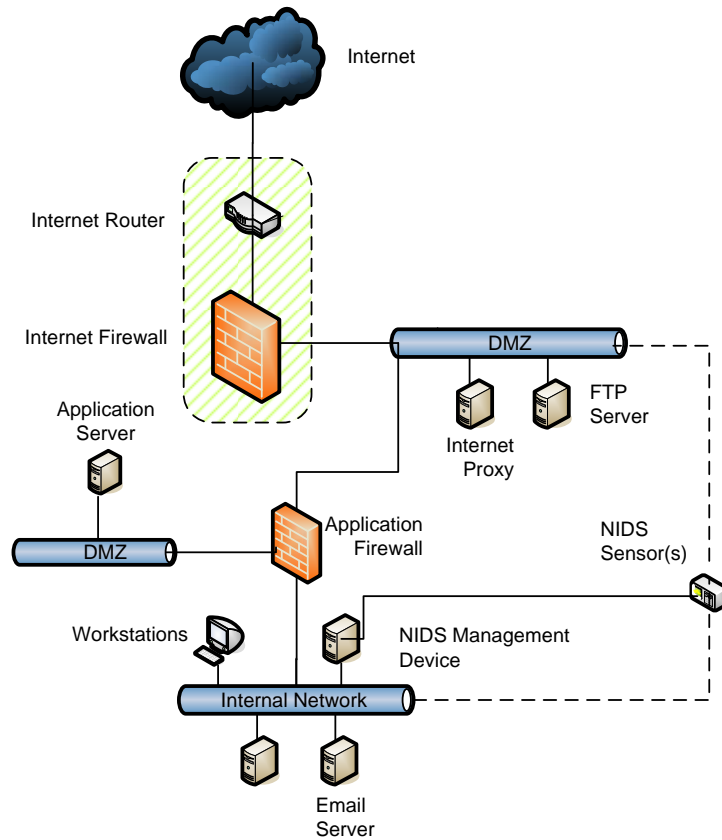


Figure 2: Internet Connection Design Pattern for Application Hosting

4.3.2 Internet Connection – Better Practice

In addition to the above good practice controls, the following better practice controls are also recommended to enhance the security level of Internet connections:

- The first point of contact from the Internet should be a network device capable of performing IP filtering (router, firewall or equivalent) that is able to discard the majority of unwanted incoming traffic
- Traffic from Internet-facing systems to non-Internet facing systems should be filtered by an application layer firewall or reverse proxy or equivalent device
- Systems in the Internet DMZ should not be configured with publicly routable IP addresses. IP masquerading should be implemented to prevent internal addresses from being translated and revealed on the Internet,
- Systems in the Internet DMZ should be split into multiple Internet DMZs based on business, sensitivity of information, functionality or other criteria based on risk assessment
- A Network Intrusion Detection System (NIDS) is utilised to monitor all systems in the Internet DMZs

4.4 Wireless Connections

It is recommended that CGIAR centers maintain a policy that internally-hosted wireless connections are segregated from internal wired networks via a minimum of one control point (not including the wireless router itself). Wireless connections should be treated as an 'untrusted' network.

4.4.1 Wireless Connection Design Pattern

The following diagram depicts the proposed CGIAR good practice approach to implementing Wireless Connection architecture at CGIAR centers.

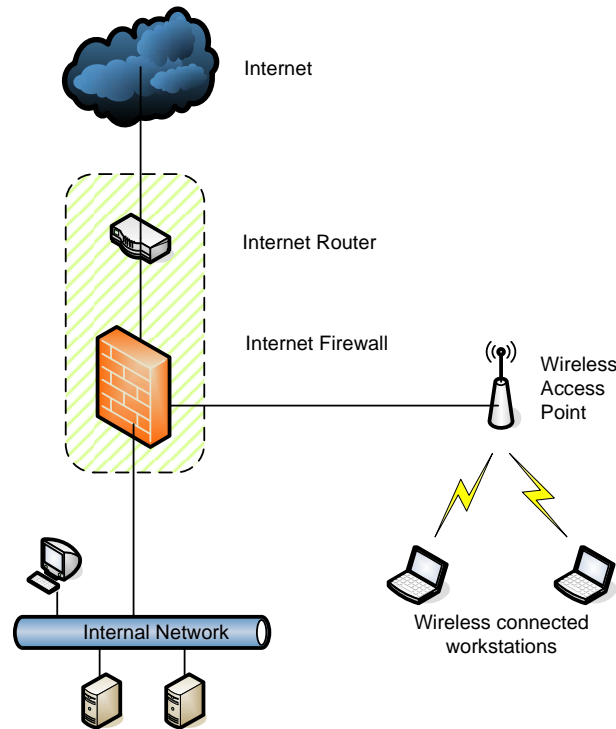


Figure 3: Wireless Connection Design Pattern

4.4.2 Wireless Connection – Good Practice

In the event of wireless networks being implemented within the CGIAR environment, a level of protection from the wireless network is required to ensure that attempts to gain unauthorised access to the CGIAR network are greatly minimised. It is recommended that the following good practice controls are adhered to:

- CGIAR center wireless networks should be physically segregated from other networks by using a transport layer firewall.
- The transmitter and receiver nodes of a wireless network mutually authenticate each other
- The center should maintain the ability to deny access to CGIAR wireless networks on a node-by-node basis
- Information transmitted over CGIAR wireless networks should be encrypted using one of the methods outlined in the wireless device configuration guidelines provided in this document at Section 5.9 or via an end-to-end VPN encryption solution
- Signal leakage should be minimised through appropriate selection of signal strength and appropriate placement of wireless access point

- Strong authentication (WPA2 Enterprise) should be implemented for all wireless clients connecting to the CGIAR network.
- In the case of visitors to CGIAR sites requiring Internet access via wireless connections, this should occur in accordance with the guideline identified in 3.8. Visitor access.

4.4.3 Wireless Connection – Better Practice

In addition to the above good practice controls, the following better practice controls are also recommended to enhance the security level of wireless networks:

- A Network Intrusion Detection System (NIDS) should monitor all traffic entering the wireless DMZ
- Users connecting to CGIAR networks using a WLAN should be authenticated by two-factor authentication.

4.5 Modem Connection

It is recommended that CGIAR centers maintain a policy that modem Connections used to access networks within CGIAR centers are to be physically segregated from those networks through the use of VLANs.

4.5.1 Modem Connection Design Pattern

The following diagram depicts the proposed CGIAR good practice approach to implementing Modem Connection architecture at CGIAR centers.

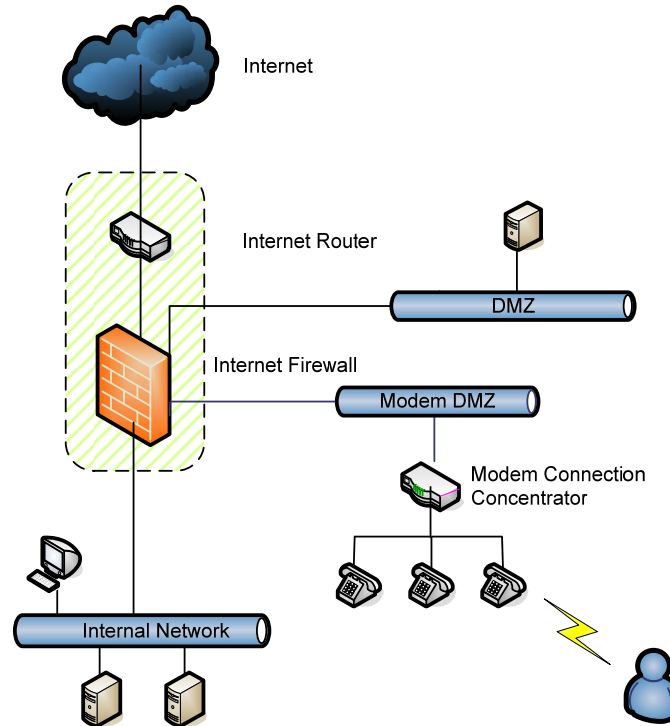


Figure 4: Modem Connection Design Pattern

- Allow access to modem connection concentrator equipment management to only authorised internal IP addresses

- Modem termination connection concentrator equipment should be patched and maintained in response to product alerts issued by the hardware or software vendor as appropriate
- Modem connection concentrator equipment should be placed in a dedicated VLAN, separated from the internal network by a firewall (either inner or Internet firewall)
- Filtering rules should be applied to allow modem users to only connect to systems they require access to for business purposes

5 NETWORK DEVICE CONFIGURATION GUIDELINES

5.1 Firewalls

5.1.1 Firewall – Good Practice

It is recommended that Centers adopt a policy that all firewalls in place within CGIAR centers should be configured in accordance with the following good practice configuration requirements:

- Implement an explicit deny rule if no other rules are matched
- All filtering rules should be implemented to only allow traffic that is in line with business operations. These rules should be configured explicitly with source, destination and network port number for each rule
- Allow device management access to only authorised internal IP addresses
- Ensure that generic logins are not used to authenticate to the firewall's administrative console.
- All communication between the management console and the firewall device is to be encrypted
- Do not include any "allow all" rules.
- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Ensure all system passwords are encrypted when stored on the device
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created.
- Firewall and perimeter security devices are to be patched and maintained on a monthly basis.
- Spoofed, invalid, or relayed packets should be rejected.
- All firewall logs should be sent to a dedicated logging server for storage and analysis purposes, with logs being retained for a minimum of 30 days.

In addition, firewall configuration and permissible service rules should not be changed unless the permission of the IT manager within the relevant center is obtained.

Testing of firewall rules should be performed on a regular basis. The testing should compare the configured rules with those that have been documented. Software tools can also be utilised to ensure that firewalls are correctly preventing the performance of operations that should be prevented.

5.1.2 Firewalls – Better Practice

The following better practice guidelines are also recommended:

- All administrative authentications to the device are to be performed via a central authentication server; for example RADIUS.

5.2 Routers

5.2.1 Router – Good Practice

It is recommended that CGIAR Centers maintain a policy that all routers in place within CGIAR centers be configured in accordance with the following good practice configuration requirements

- Where the router sits on a trust boundary or other logical network boundary, implement Access Control Lists (ACLs) to limit communications between networks
- Ensure all system passwords are encrypted when stored on the device
- Ensure that generic logins are not used to authenticate to the router's administrative console.
- Allow device management access to only authorised internal IP addresses
- All communication between the management console and the routers is to be encrypted
- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created.
- Disallow all of the following:
 - IP directed broadcasts
 - Incoming packets at the device sourced with invalid addresses such as RFC1918 address
 - TCP small services
 - UDP small services
 - All source routing
 - All web services running on device
- Routers are patched and maintained according to the following:
 - Every 3 months for routers providing connectivity to external networks
 - Every 6 months for routers that are not connected to external networks
- All router logs should be sent to a dedicated logging server for storage and analysis purposes, with logs being retained for a minimum of 30 days.

5.2.2 Router – Better Practice

The following better practice guidelines are also recommended:

- All administrative authentications to the device is to be performed via a central authentication server such as RADIUS
- All router logs should be sent to a dedicated logging server for storage and analysis purposes

5.3 Bandwidth Accelerator / Prioritisation Devices

5.3.1 Bandwidth Accelerator / Prioritisation Devices – Good Practice

It is recommended that CGIAR centers maintain a policy that all bandwidth accelerator / prioritisation devices in place within the center be configured in accordance with the following good practice configuration requirements

- Ensure all system passwords are encrypted when stored on the device
- Ensure that generic logins are not used to authenticate to the device's administrative console.

- Allow device management access to only authorised internal IP addresses
- All communication between the management console and bandwidth accelerator / prioritisation devices is to be encrypted
- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created
- Bandwidth accelerator / prioritisation devices are patched and maintained according to the following:
 - Every 3 months for bandwidth accelerator / prioritisation devices providing connectivity to external networks
 - Every 6 months for bandwidth accelerator / prioritisation devices that are not connected to external networks
- Ensure that all network services required for business purposes are granted higher priority over those that are not required

5.4 Modem Concentrator Devices

5.4.1 Modem Concentrator Devices – Good Practice

It is recommended that CGIAR Centers maintain a policy that all modem concentrator devices in place within CGIAR centers be configured in accordance with the following good practice configuration requirements

- Ensure all system passwords are encrypted when stored on the device
- Ensure that generic logins are not used to authenticate to the device's administrative console.
- Allow device management access to only authorised internal IP addresses
- All communication between the management console and the modem concentrator devices is to be encrypted
- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created.
- Modem concentrator devices are patched and maintained according to the following:
 - Every 3 months for routers providing connectivity to external networks
 - Every 6 months for routers that are not connected to external networks
- Ensure that all unused modem ports are disabled
- Ensure that all users who are connecting to the CGIAR network through modem access are appropriately authenticated before being granted access
- Ensure appropriate filtering is implemented so modem users can only access systems they require for business purposes

5.5 Content Filters

5.5.1 Content Filters – Good Practice

It is recommended that the following good practice controls are adhered to with respect to every content filter installation within CGIAR centers:

- Content filters should use a combination of “black lists” and “white lists”
- Content filters should be patched and maintained according to vendor security advisories
- Signatures of content filters should be updated on a daily basis
- A report documenting filter activity (in particular, attempts to access unauthorised material) should be generated on a daily basis and reviewed by the IT Manager.

Content filters should be used to block access to material that is considered inappropriate (for example, pornography) – further guidance on this is available in the Internet Security and Acceptable Use Good Practice Guide. Policies as to what constitutes acceptable content may be determined by center management rather than the IT manager specifically.

5.6 LAN Switches

5.6.1 LAN Switches – Good Practice

It is recommended that the following good practice controls are adhered to with respect to every layer 2 switch in place within CGIAR centers:

- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Allow device management access from only authorised internal IP addresses
- Ensure all system passwords are encrypted when stored on the device
- Ensure that generic logins are not used to authenticate to the switch’s administrative console
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created.
- Switches are to be patched and maintained on a bi-annual basis
- Ensure all unused switch ports are configured into a shutdown state
- All switch logs should be sent to a dedicated logging server for storage and analysis purposes, with logs being retained for a minimum of 30 days.

It is also recommended that switches that implement layer 2 Virtual Local Area Networks (VLANs) comply with these good practice requirements:

- Disable the use of VLAN trunking configuration on switch ports that do not require this configuration
- When using trunking on network ports, the trunking protocol should be defined. Do not allow the switches to negotiate trunking protocols
- Avoid bridging two or more VLANs together. If communication is required between VLANs, a layer 3 switch should be implemented and routing enabled

5.6.2 LAN Switches – Better Practice

The following better practice guidelines are also recommended:

- All network ports listed in the switch configuration (when accessing the switch console) are to be configured with a description of the device connected
- All administrative authentications to the device is to be performed via a central authentication server such as RADIUS
- A VLAN should be implemented on all network switches to support administrative functions

5.7 Network Intrusion Detection/Intrusion Prevention Systems

5.7.1 Network Intrusion Detection/Prevention Systems – Good Practice

It is recommended that CGIAR centers maintain a policy whereby, if a CGIAR center hosts a web server or any other server that is externally accessible, a Network Intrusion Detection or Prevention System device is in place which meets the following good practice guidelines:

- Restrict management access to only authorised internal IP addresses
- All communication between the management console and the device is to be encrypted
- The network interfaces being used for monitoring and network traffic collection should not be configured with an IP address
- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created.
- Signatures must be updated on a daily basis or as available
- Devices are to be patched and maintained in response to operating system and product alerts issued by the respective vendors

5.7.2 Network Intrusion Detection/Prevention Systems – Better Practice

The following better practice guidelines are also recommended:

- Tune the alerting levels to suit the specific infrastructure hosted within each center (this can be achieved with an IPS by running it in passive mode when the device is initially implemented). For example, if a Microsoft IIS web server is being hosted within a center, alerts should be disabled for Apache or other web server products as they are not relevant for the IIS web server

5.8 Antivirus

which contains the following antivirus configuration requirements.

5.8.1 Antivirus – Good Practice

It is recommended that CGIAR centers maintain a policy putting in place the following antivirus measures:

- Antivirus gateways are implemented to monitor outgoing and incoming web and email traffic for suspicious activity that may be suggestive of the existence of a virus or other malware. Alternatively, monitoring of web and email traffic for viruses can be outsourced to a trusted and reliable 3rd party.
- Network connections from workstations in CGIAR to internal networks to the Internet should be blocked to prevent the spread and activation of malware (legitimate network traffic such as web and email must be routed through a proxy in the DMZ).

5.9 Wireless Access Points

5.9.1 Wireless Access Points – Good Practice

It is recommended that CGIAR centers maintain a policy that wireless access points within CGIAR centers meet the following good practice guidelines:

- The administrative console must not be available via the wireless radio network
- Wireless Access Points are to be patched and maintained in response to product alerts issued by the hardware vendor
- Strong encryption should be used by all clients connecting to the Wireless Access Point (example of encryption methods include WPAv2, WPAv1)
- All wireless networks should be terminated in a separate VLAN. Strong authentication in the form of the 802.1x standard should also be utilised.

5.10 VPN Devices

5.10.1 VPN Devices – Good Practice

It is recommended that CGIAR centers maintain a policy that VPN devices within CGIAR centers which are dedicated or also include routing and firewall functionality should meet the following good practice guidelines:

- Allow VPN device management access to only authorised internal IP addresses
- VPN devices should be patched and maintained in response to product alerts issued by the hardware or software vendor as appropriate
- VPN devices should be placed in a dedicated DMZ
- Filtering rules should be applied to allow VPN users to only connect to systems they require access to for business purposes only

5.10.2 VPN Devices – Better Practice

- VPN devices should be configured to only accept connections using Layer 2 Tunneling Protocol with IPSec

5.11 Web Proxy Servers

5.11.1 Web Proxy Servers – Good Practice

It is recommended that CGIAR centers maintain a policy whereby proxy servers implemented for use in CGIAR centers comply with the following good practice configuration guidelines:

- Allow proxy server management access to only authorised internal IP addresses
- Each proxy should only be configured to permit the flow of traffic in a single direction
- Proxies are patched and maintained in response to product alerts issued by the operating system and proxy software vendor.
- All proxy users should be forced to authenticate before access to Internet and other related services are permitted. In the event of authentication not being feasible in some cases, access rules should be implemented to cater for these connections.

5.11.2 Proxy Servers – Better Practice

The following better practice guidelines are also recommended:

- Disallow use of proprietary protocols

5.12 VoIP Gateway

5.12.1 VoIP Gateway – Good Practice

It is recommended that CGIAR centers maintain a policy whereby every VoIP gateway in place within CGIAR centers should adhere to the following good practice guidelines:

- Allow VoIP gateway management access to only authorised internal IP addresses
- All management access traffic should be encrypted.
- Ensure that the system passwords meet the following requirements:
 - Minimum of 8 characters
 - A combination of uppercase and lowercase characters, numbers, and other special characters
- Ensure that a minimum of 2 non-generic accounts with administrative privileges are created.
- Do not allow external access to the internal user registrar configured in the VoIP system
- Disable all unnecessary functionality
- VoIP gateways should be patched and maintained as per product alerts issued by the gateway vendor

5.12.2 VoIP Gateway – Better Practice

The following better practice guidelines are also recommended:

- Encrypt VoIP sessions

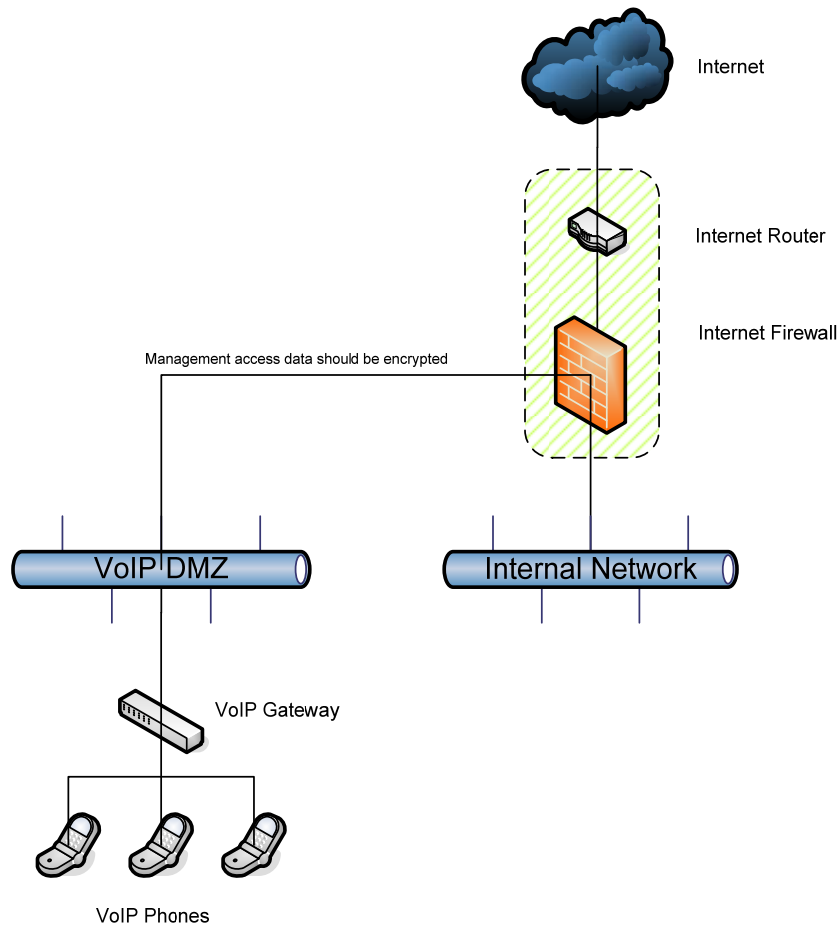


Figure 5: VoIP Connection Design Pattern

6 APPENDIX A: DEFINITIONS

Access Control List (ACL): A file used to determine a users' individual access rights and privileges to folders / directories and files on a given system. Common privileges include allowing a user to read a data item; read a file or part of a file (or all the files in a folder/directory); to write/update/delete the file or files, and to run (execute) the file (if it is an executable file, or program).

Administrative Console: The interface from which an administrator can set configurations or perform privileged tasks to a given system. Administrative consoles will often be restricted in usage to only specific privileged users.

Authentication: The process of identifying an individual, usually based on a username and password. Authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Three types of factors are used to provide authentication: a) something you know [eg a password], b) something you have [e.g. a certificate or card], and c) something you are [eg a fingerprint or retinal pattern]. Using any two in conjunction is known as two-factor authorization.

Captive Portal: Refers to a security tool that forwards users of publicly accessible networks to a web page where they are forced to provide authentication credentials before they are able to access particular functionality (for example, Internet access) is made available. Captive portals can also be used to control bandwidth use by limiting the speed and / or size of data that can be uploaded and downloaded.

Challenge / Response: Used in authentication, the challenge / response protocol will issue a challenge which theoretically will only be known by authorised users or devices.

Demilitarized Zone (DMZ): A separate part of the Center's network that is shielded and "cut-off" from the main LAN network and its systems. The DMZ prevents external parties from gaining access to your internal systems.

Development Environment: The systems or environment used by an organisation for development of new systems, applications or otherwise. Development environments may be physically and logically separated from other environments.

Dial-up: A telephone service is used to communicate with a computer.

Firewall: A security device (both hardware and software) that is used to restrict access in communication networks. They prevent unauthorised computer access between networks, or networks and applications, and only allow access to services that are expressly registered. They also keep logs of all activity, which may be useful in investigations.

Hardware Tokens: Hardware tokens are physical devices utilised to authenticate the validity of users.

Host: An intelligent device that stores or processes information in various forms, which should be configured or managed regardless of whether an end-user interacts directly with the device.

Malware: Refers to malicious software commonly spread via public networks, such as the WWW.

Modem Connection Concentrator Equipment: Refers to a device that serves as a central point through which modem connections made to CGIAR centers can be directed and managed

Network Intrusion Detection Systems: Or NIDS is an intrusion detection system that resides on the internal network of an organisation. The NIDS attempts to detect malicious activity by observing traffic around the network via sensors placed at key points in the network. NIDS can inspect both incoming and outgoing traffic for suspicious activity or data.

Network Services: Network services are generally a set of functions installed on servers in a network which provide shared resources across the network. These include services such as DNS, email, printing, directory services, authentication and others.

Privileged Access Control System: Also called network access control (NAC), is a method of bolstering network security by restricting the availability of network resources to endpoint devices that comply with a

defined security policy. A traditional NAC performs authentication and authorisation functions for potential users by verifying logon information. In addition to these functions, NAC restricts the data that each particular user can access, as well as implementing anti-threat applications such as firewalls, antivirus software, and spyware-detection programs. NAC also regulates and restricts the things individual users can do once they are connected.

Production Environment: The systems or environment in which live data, processing or storage of organisation, business or research information occurs.

Public Information: The lowest information asset classification and has been explicitly approved in writing by the Center's management for release to the public.

RADIUS: Remote Authentication Dial in User Service (RADIUS) is a network protocol which provide access, authorisation and accounting management controls.

Restricted Information: The most sensitive form of information asset. This information requires some protection and is not generally available internally.

Router: A router is a device utilised to route or forward data between two separate networks.

Secure Sockets Layer (SSL): SSL provides a method of authenticating the communicating parties (client and server authentication) and encrypting the information exchange between those parties. SSL is supported by most web browsers and web servers.

Sensitive Information: Information assets classified as restricted, confidential or internal use.

Trojan Horses: Potentially damaging unauthorized code hidden within authorized programs.

Test Environment: The environment in which systems are tested. These environments are often separated from production and development environments due to the unstable nature of pre release applications, or new applications and systems.

Trust Boundary: A trust boundary is a physical or virtual demarcation point separating different levels of trust. That is, where the "trustworthiness" of entities changes from one side of the boundary to the other.

Viruses: An unauthorized program that replicates itself, attaches itself to other programs and spreads onto various data storage media or across the network. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification data for files, increased file sizes, and a possible total failure of the infected computer.

Virtual Private Network (VPN): A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. A defining feature is that all communication is encrypted.

Virtualisation: Refers to the masking of server resources, including the number of individual physical servers and operating systems, through use of special software applications to divide individual physical servers into multiple separated virtual environments. Each virtual environment appears to end users to exist as discrete physical machines.

VLANs: A virtual LAN, a network of computers physically connected to the same switch or set of switches but configured as a logically separate network which should not be visible to devices on other VLANs unless otherwise specified.

Web Proxy: A web proxy is utilised to connect Internet resources between clients and servers. Often the web proxy will be utilised as a cache and to provide content filtering (blacklisting).

WPA: Wi-Fi Protected Access compliant wireless devices implement a security protocol capable of strong authentication controls. WPA is a premature implementation of the advanced WPA2.

7 APPENDIX B: CHECKLISTS

The following checklists are designed to assist CGIAR centers that wish to adopt any or all of the good and better practices listed in this document. The checklists should be used by a center when attempting to assess their level of current adherence with the guidelines listed in this document. This will allow any gaps with good and better practices to be identified, after which centers can assess whether addressing those gaps will be feasible.

7.1 Good Practice Checklist

Guideline Number	Guideline Name	Tick if center currently adheres to this guideline
Section 3 - Internal Network Architecture		
3.1	Internal LAN requirements	<input type="checkbox"/>
3.2	Security of Network Services	<input type="checkbox"/>
3.3	Storage of sensitive information on Networked Systems	<input type="checkbox"/>
3.4	Network Connection Control	<input type="checkbox"/>
3.5	Administrative Services	<input type="checkbox"/>
3.6	Networks supporting Test and Development environments	<input type="checkbox"/>
3.7	Documentation of network configuration and architecture	<input type="checkbox"/>
3.8	Visitor access	<input type="checkbox"/>
3.9	Access to internal applications	<input type="checkbox"/>
3.10	Virtualized Environments	<input type="checkbox"/>
Section 4 – External Connection Guidelines		
4.1	Third Party Access to Internal Networks	<input type="checkbox"/>
4.2	User Authentication for External Connections	<input type="checkbox"/>
4.3	Segregation of Internet Connections	<input type="checkbox"/>
4.3.1	Internet Connection – Good Practice	<input type="checkbox"/>
4.4	Wireless Connections	<input type="checkbox"/>

Guideline Number	Guideline Name	Tick if center currently adheres to this guideline
4.4.1	Wireless Connection Design Pattern	<input type="checkbox"/>
4.4.2	Wireless Connection – Good Practice	<input type="checkbox"/>
4.5	Modem Connection	<input type="checkbox"/>
4.5.1	Modem Connection Design Pattern	<input type="checkbox"/>
Section 5 – Network Device Configuration Guidelines		
5.1.1	Firewalls – Good Practice	<input type="checkbox"/>
5.2.1	Routers – Good Practice	<input type="checkbox"/>
5.3.1	Bandwidth Accelerator / Prioritisation Devices – Good Practice	<input type="checkbox"/>
5.4.1	Modem Concentrator Devices – Good Practice	<input type="checkbox"/>
5.5.1	Content Filters – Good Practice	<input type="checkbox"/>
5.6.1	LAN Switches – Good Practice	<input type="checkbox"/>
5.7.1	Network Intrusion Detection Systems – Good Practice	<input type="checkbox"/>
5.8.1	Antivirus – Good Practice	<input type="checkbox"/>
5.9.1	Wireless Access Points – Good Practice	<input type="checkbox"/>
5.10.1	VPN Devices – Good Practice	<input type="checkbox"/>
5.11.1	Web Proxy Servers – Good Practice	<input type="checkbox"/>
5.12.1	VoIP Gateway – Good Practice	<input type="checkbox"/>

7.2 Better Practice Checklist

Guideline Number	Guideline Name	Tick if center currently adhere to this guideline
3.4.1	Network Connection Control – Better Practice	<input type="checkbox"/>
4.3.2	Internet Connection – Better Practice	<input type="checkbox"/>

Guideline Number	Guideline Name	Tick if center currently adhere to this guideline
4.4.3	Wireless Connection – Better Practice	<input type="checkbox"/>
5.1.2	Firewalls – Better Practice	<input type="checkbox"/>
5.2.2	Routers – Better Practice	<input type="checkbox"/>
5.6.2	LAN Switches – Better Practice	<input type="checkbox"/>
5.7.2	Network Intrusion Detection Systems – Better Practice	<input type="checkbox"/>
5.10.2	VPN Devices – Better Practice	<input type="checkbox"/>
5.11.2	Proxy Servers – Better Practice	<input type="checkbox"/>
5.12.2	VoIP Gateway – Better Practice	<input type="checkbox"/>

8 DOCUMENT CONTROL

Version Control Log

Version	Description	Date
1.00	Third draft following additional feedback	18 Jun 2009
1.10	First published edition	24 Aug 2009

Copyright & Legal

This guideline, prepared specifically for **Consultative Group for International Agricultural Research**, is the intellectual property of SIFT Pty Limited. When finalised, SIFT Pty Limited authorises CGIAR to reproduce or disseminate this guideline as necessary to further the aims and goals of CGIAR, under a Creative Commons Attribution-Noncommercial-Share Alike 2.5 Australia License

In no event shall SIFT Pty Limited be liable to anyone for special, incidental, collateral, or consequential damages arising out of the use of this information.

SIFT® is a Registered Trademark of SIFT Pty Ltd. Many designations used by manufacturers and sellers to distinguish their products are claimed as trademarks or other proprietary rights. Where designations appear, and when the editorial staff were aware of a claim, the designations have been shown. Other trademarks, registered trademarks, and service marks are the property of their respective owners.

Copyright © 2009 SIFT Pty Limited. Originated in Australia.

The first published version provided by SIFT Pty Limited, and future versions with modifications made by the CGIAR, as coordinated through the CGIAR ICTKM Program and the CGIAR Internal Auditing Unit, are being distributed by these Units in accordance with the terms of the above license, which can be found at <http://creativecommons.org/licenses/by-nc-sa/2.5/au/> "