Ministry of Communications & Information Technology

Network Infrastructure Configuration Standard

Table of Contents

1. Introduction

1.1 Background

In an interconnected world, network security plays a vital role in determining who and what is provided access into and out of the Government of Samoa's (GoS) Information and Communication Technology (ICT) environment. At the same time, each GoS agency needs to facilitate access to its staff, partners, suppliers, customers and also to the essential technology platforms that allow this to happen. By carefully implementing a number of controls, GoS can be confident that providing access does not adversely impact the security of its systems and the important information assets it holds.

1.2 Purpose and Scope

These standard details the GoS approach to maintaining a strong security posture for its network assets and provides baseline security requirement for all the systems and components that we own, operate and maintain. This also extends to networks that might be managed on our behalf by external partners who store, handle or process our data.

The Scope of the Network Infrastructure Configuration Standard includes all technologies that provide networking / interconnect services for the GoS IT environment, including third party hosting providers. Additionally, the scope of this standard includes servers within the GoS IT environment, by way of their required positioning and network exposure and use.

2. Principle

The following principles underpin our approach to ensuring the secure management and configuration of all network infrastructure.

Principle	Description
Set up a baseline level of device security for network equipment.	All devices must be hardened before deployment on to the network. This involves a formal configuration process to ensure all devices meet a minimum state of security – e.g., in terms of open ports, available network services are minimised to what is necessary for business purposes, etc.
Connection to GoS networks limited to authorised devices.	Only devices which are managed by the GoS and/or are known to be secured can be connected to GoS networks. If the device is not directly managed by the GoS control and management via Device Management (aka MDM) is permissible.

Protect what you can, detect everything else.	Networks and/or endpoints shall be monitored continually to detect unauthorised connections and suspicious traffic.
3rd party access to GoS systems and data to be governed by secure processes.	For situations where 3rd parties are able to access or modify GoS systems, data or networks, agreements and processes must be in place to ensure that GoS can be confident its security is not put at increased risk through these arrangements.

3. Requirements

3.1 Localised Networking Requirements

Localised networks are a key conduit to enable our staff to undertake their work (whether they connect through a physical connection or Wi-Fi), and in delivering effective services to our customers and partners. So, we need to protect these networks from potential compromise as effectively as possible by making sure they are configured and used securely.

Requirement	Description
Network architecture and configuration details must be documented and maintained	The GoS network architecture and configuration must be documented, and this documentation maintained to ensure accuracy.
Internal networks must segregate systems of different sensitivity levels, and wired from wireless networks	Wireless networks must be segmented from wired networks.
	Internal networks within GoS must be configured to segregate different types of systems, or systems hosting information of differing sensitivities, by use of (Virtual LAN) VLANs and the creation and management of isolated security domains. All Traffic between zones of different sensitivity must traverse a firewall.
	Development and test environments must be logically segregated from production networks to prevent information leakage or unauthorised access.
System clocks must be synchronised with an NTP provider	All system clocks must be synchronised with a certified Network Time Protocol (NTP) provider via internal intermediary time servers, and modification of system clock times must be prevented.

3.2 Cloud Requirements

The use of cloud services increasingly forms part of the way we deliver our services, as these services offer us the ability to support the delivery of efficient, reliable and scalable services. However, it is important that cloud services are managed securely.

Requirement	Description
Cloud services must be used and configured securely	Multi-factor authentication must be used for management / administrative level access to Cloud based resources.
	A federated identity management solution must be used to effectively manage the various accounts staff within GoS agencies use to access cloud-based services
	Sensitive data must be encrypted while in transit and when stored in cloud environments (many cloud services offer in-built encryption by default – this is acceptable provided the encryption used is considered to meet current industry best practice).
	Agreements with the Cloud Service Provider(s) (CSP) should incorporate the following: • GoS's ownership of data, including provisions for recovery of the data in the event of CSP bankruptcy or similar. • SLAs for availability including compensation. • Independent audit and assurance activities for controls. • Compliance with the customer's privacy obligations. • Physical locations of data storage centres and global CSP infrastructure backups
	For situations where a cloud service GoS agency relies on is unavailable for a period of time, a Business Continuity and Disaster Recovery Plans must be invoked.

3.3 Security Assurance and Testing

To ensure continued confidence that our networks are as secure as they can be, a number of assurance activities must be scheduled and undertaken on a regular basis.

Requirement	Description
Security Testing must be conducted on GoS's networks on a regular basis	Security testing must be conducted against GoS networks (both internal and external facing) network regularly, with the frequency of testing determined based on the level of risk associated with that network. This includes:

	• Whether particularly sensitive systems are connected to the network (which would increase the frequency of testing); and • When there is any significant change to the network environment. Security testing and assurance activities may include: • Quarterly internal and external vulnerability scanning. • Vulnerability scanning of systems after changes have been implemented. • Annual penetration testing. • Ad hoc Penetration testing following major changes, or the implementation of new services.

3.4 Network Infrastructure – Build Requirements

The following requirements apply to all GoS network infrastructure builds.

Requirement	Description
All network infrastructure must be built and documented using an industry accepted security baseline	All network infrastructure builds must be completed and documented based upon industry and vendor-specific best-practice guidelines. For example: • Center for Internet Security (CIS) Benchmarks[1] • Windows Security Baselines[2] • Cisco IOS Device Hardening Guide[3]
	This standard takes precedence if there are conflicts with the above sources unless an exemption is granted by the SamCERT team, and the details of the exemption are recorded in the risk register.
	The SamCERT team must be consulted with, if a hardening standard doesn't exist for a chosen platform or technology to determine appropriate build requirements.

[1] https://www.cisecurity.org/cis-benchmarks/
[2] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
[3] https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

3.5 Network Infrastructure – Configuration Requirements

To achieve a secure network environment that offers the best possible protection against potential breaches, data compromise, fraud or theft, all GoS network infrastructure are requried to be configured and managed as follows:

Requirement	Description
All network infrastructure must meet the following security requirements	All network infrastructure must have a documented business purpose and designated system/platform owner.
	Vendor default passwords/secrets for network infrastructure must be changed prior to implementation and deployment into production.
	An authentication server (e.g. RADIUS, LDAP or TACACS+) must be used to centralise and control all administrator level access to network infrastructure.
	Where applicable, management interfaces must be configured to time out logged-in sessions after a predetermined period
	Passwords for accessing network infrastructure devices must conform to security requirements.
	Default access to management protocols such as SNMP must be modified before devices are placed into production. Read-only SNMP community strings must be changed from defaults to provide less environmental insight to a would-be-attacker. If SNMP is required, older versions of the protocol such as SNMP V1 and V2 must be avoided wherever possible.
	"Break-Glass" accounts must be commissioned to cater for central authentication server failure.
	Credentials stored on each component device must be encrypted.
	Access to management interfaces must be restricted to a dedicated network zone.
	Management activities must be performed solely over encrypted protocols.
	All network infrastructure must have logging functions enabled, with logs transmitted to a centralised logging server in accordance with the *Log Management and Monitoring Standard.*
	Where practicable: • Configuration management tools should be used to maintain and facilitate changes to device configurations. • Device configuration backups and archives must be stored securely, with access limited to the same personnel that have access to manage devices

	• Network device configurations should be monitored for unauthorised changes through the aforementioned tools, or by using automated tools such as RANCID[4] or Oxidized[5]
	Network infrastructure must be patched regularly to address any security vulnerabilities in accordance with the *Patch and Vulnerability Management Standard*.
	All network device configurations must be checked annually against an accepted baseline to ensure that they are compliant with this standard. Any deviations from the standard must either be rectified or included in the SamCERT risk register.

3.6 Servers – Requirements

Servers are critical to the operation of the GoS. They fulfil a wide-range of roles from data processing and storage, to authentication and business-critical functions like email and collaboration. For this reason, strong controls must be implemented that govern their secure operation.

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, Servers must meet the following requirements	All servers must be configured to a Standard Operating Environment (SOE) that conforms with vendor and industry-accepted hardening standards.
	All firmware and software must be updated to the latest available version as per the *Patch and Vulnerability Management Standard*, prior to deployment of servers into production.
	Resources used to build server operating systems (scripts, build servers, configuration management systems, image files) must be adequately secured and monitored to prevent source compromise.
	Servers must employ the use of a host-based firewall.
	Only network services, protocols and ports with a defined business requirement are to be enabled.
	All servers must have anti-malware software installed as per the *Malicious Code Standard*.
	All functions, for which there is no business requirement, are to be uninstalled or disabled, including drivers, subsystems, file systems, scripts, and other features
	Servers must be housed in a physically secure location, as per the GoS agencies' Physical Security Standards/requirements.

[4] http://www.shrubbery.net/rancid/
[5] https://github.com/ytti/oxidized

	Read Only Domain Controllers (RODC) must be used where the physical security of the domain controller cannot be guaranteed, for example in smaller branch offices without a secure comms room.

3.6.1 Routers - Requirements

Routers form the backbone of the GoS networks. For this reason, strong controls must be implemented that govern their secure operation.

Note: The nature of a network standard such as this is to define the high-level principles which govern the approach to network security within your organisation. The specific, low-level configuration requirements for your infrastructure will ultimately depend on your level of cyber risk, and the type, make and model of routers you have in place. A suggested starting point for configuration of routers is provided in this table, but this should be supplemented by your own assessment of relevant configuration requirements[6].

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, routers must meet a range of secure configuration requirements.	All 'allowed' traffic must have a defined and documented business requirement
	Access Control Lists (ACLs) must be implemented where a router controls traffic between networks of differing trust levels
	Wherever practicable, <Company Name> must implement all available security features for the operative routing protocol. These may include, but are not limited to: • BGP/OSPF TTL Security Check • Control Plane Policing & Protection • Default passive interface • iACLs, rACLs • Neighbour Authentication • Routing peer definition
	Routers must be configured to disallow the following: • IP directed broadcasts • Packets with incongruous or invalid addresses (e.g. RFC1918/IPv4 from external source addresses) • TCP and UDP small servers or Daemons (e.g. Echo, Discard)

[6] Examples of guides that may be able to assist further with configuration of routers are numerous. See for instance these resources from Cisco and the Centre for Internet Security:
https://tools.cisco.com/security/center/resources/securing_nx_os.html,
https://tools.cisco.com/security/center/resources/increase_security_ios_xr_devices.html
https://www.cisecurity.org/cis-benchmarks/

	• All source routing • Web services for router administration • Telnet, FTP, and HTTP services • Auto-configuration
	If HSRP (Hot Standby Router Protocol) or similar redundancy protocols are in use, the configuration must implement measures to prevent rogue routers from being introduced for Denial of Service (DoS) or Man in the Middle (MITM) attacks[7]

3.6.2 LAN Switches - Requirements

Similar to routers, LAN (Layer 2) switches are hardware-based components that allow traffic to traverse the network and are required to be securely configured.

Note: The nature of a network standard such as this is to define the high-level principles which govern the approach to network security within your organisation. The specific, low-level configuration requirements for your infrastructure will ultimately depend on your level of cyber risk, and the type, make and model of switches you have in place. A suggested starting point for configuration of switches is provided in this table, but this should be supplemented by your own assessment of relevant configuration requirements[8]

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, LAN switches must meet the following requirements	All rules impacting switch traffic allowed must include a comment that clearly states the purpose / intent of the rule
	All network ports in use must be configured to include a description of the connected device type wherever practicable (for access layer switches, a generic description may be suitable (e.g. printer, access point etc))
	Unused switch ports must be disabled or placed in a non-routable VLAN
	For switches which implement layer 2 Virtual Local Area Networks (VLANs): • Dynamic Trunk protocol must be disabled[9] • Switches must not be able to negotiate their own trunking protocol - trunking protocols must be defined.

[7] https://portunreachable.com/exploiting-cisco-hsrp-63bd45f9af58

[8] Examples of guides that may be able to assist further with configuration of switches are numerous. Cisco for example has configuration guides available for a range of switches - https://www.cisco.com/c/en/us/support/switches/index.html.
See similarly Juniper Networks for documentation relevant to their range of switches - https://www.juniper.net/documentation/.

[9] http://packetlife.net/blog/2008/sep/30/disabling-dynamic-trunking-protocol-dtp/

	• VLANs must not be bridged together using layer 2 switches - a layer 3 (destination/IP based) switch must be implemented, and routing enabled
	Discovery protocols such as Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP): • On internal interfaces: Must be disabled if unneeded • On outward-facing interfaces: Must be disabled • Access to CDP tables can lead to unwanted mapping/discovery of the entire network topology.
	Dynamic ARP Inspection (DAI) must be enabled[10] to combat ARP Spoofing attacks
	DHCP Snooping[11] must be configured (if available) to mitigate the threat of rogue DHCP servers

3.6.3 Firewalls – Requirements

Firewalls guard the perimeter of our network environments and protect GoS systems against external threats and attacks. Configuring firewalls correctly to face a rapidly changing threat landscape is an important component of the GoS's overall security effort.

Note: The below table provide a starting point for appropriate configuration requirements for firewalls. You can access more detailed guides to supplement this standard from a range of resources, based on your organisation's needs. See for example the NIST Special Publication 800-41 Guidelines on Firewalls and Firewall Policy at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf and the Cisco Firewall Best Practices Guide at https://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, Firewalls must meet the following requirements	There must be an explicit 'deny all if no other rules are met' rule included in the firewall
	Each rule in the firewall must be configured with source, destination, and network port numbers
	Each rule in firewalls must include a comment defining the purpose of the rule and the associated change request
	'Allow all' or 'And (source) Any (protocol) Any (destination)' rules must not be permitted in firewalls

[10] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dynarp.html
[11] https://packetpushers.net/five-things-to-know-about-dhcp-snooping/

	Spoofed, invalid, or relayed packets must be rejected
	Where traffic volumes are too significant to permit effective review, the following must be prioritised for logging: • Inbound rejected traffic • Unusual outbound traffic
	All allowed traffic must have a valid business requirement

3.6.4 Content and Proxy Filters - Requirements

Devices attached to *GoS* network use applications and may, in some cases, connect to the Internet. *GoS agencies* may use a combination of both proxy filters and dynamic content filters.

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, Content Filters and proxies must meet the following requirements	Dynamic content filters must operate with the ability to block, log and filter websites based upon specific categories.
	Signatures for content filters must be updated daily
	Reports of filtered content must be reviewed frequently, as per each organisations business requirements
	All traffic from GoS's networks to the Internet must traverse organisations' proxy server(s), with any exceptions recorded in the SamCERT risk register
	All proxy users must connections to the proxy service must be authenticated prior to being able permitted to access the Internet or related services. Any exceptions must be documented in the SamCERT risk register
	All unnecessary ports and services for proxies must be disabled.
	Reports of filtered content for proxies that are serving as content filters must be generated and reviewed daily
	The use of the WPAD protocol should be avoided if possible.[12] [13]
	Access to configuration such as PAC files hosted apart from the proxy service must be appropriately secured to prevent malicious tampering

[12] http://www.trendmicro.co.uk/media/misc/wp-badwpad.pdf
[13] https://support.microsoft.com/en-us/help/3165191/ms16-077-security-update-for-wpad-june-14-2016

3.6.5 IDS/IPS, WAF, FIM, SIEM - Requirements

In addition to firewalls that protect the edges of our network; Intrusion Detection/Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM) are behavioural security applications that we may use to continually scan network traffic for anomalous behaviour that might represent a threat to our systems.

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, IDS/IPS, File Integrity Monitoring, and SIEM systems must meet the following requirements	Network interfaces used for monitoring and collecting network traffic must not be configured with an IP address
	Logs collected as part of IDS/IPS, FIM or SIEM must meet the requirements of the *Log Management and Monitoring Standard*
	Active scanners used as part of IDS/IPS, FIM or SIEM must autonomously resolve any identified security issues wherever possible/practicable
	Signature files must be updated as soon as is practicable after they become available
	Log gathering endpoints must be implemented within each zone – i.e. where the trust levels change
	Where it does not introduce operational risk, IPS's must be configured to block malicious traffic
	SIEM/correlation policies must be established which reflect real threats to the organisation and likely attack vectors
	SIEM/Correlation policies must be reviewed and tuned regularly to ensure indicators of compromise can be effectively detected
	Standard Operating Procedures, including triage processes and related service level agreements (SLA) must be documented and implemented to support timely resolution of issues arising

3.6.6 Wireless Network Configuration - Requirements

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, wireless devices and	Administrative interfaces for wireless or other network devices must not be accessible via wireless networks
	Appropriate encryption must be enforced according to the intended purpose of each wireless network. For example: 1. Guest networks – WPA2 PSK (Pre-Shared Key), where the PSK is rotated regularly

networks deployed within <Company Name> must meet the following requirements	2. Internal networks – Strong encryption (such as WPA2 with FIPS compliance enforced[14]) with EAP-TLS or similar, combined with a centralised authentication service (RADIUS)
	Wireless networks must be segmented from wired networks by a firewall. For example, guest access to the wireless access points must be configured to prevent access to the corporate network environment
	Wireless networks in different security zones must be segmented from one another by a firewall.
	Wireless network devices must be configured to detect and where possible block rogue devices
	Where possible, the signal strength for wireless access points should be limited to avoid excessive 'signal bleed' beyond the physical perimeter
	SSIDs for wireless networks other than Guest networks must not identify GoS
	Wireless scanning must be undertaken annually to confirm that only authorised wireless access points have been connected to the network
	Wireless Access Point and Controller firmware must be kept up-to-date
	Wireless access points must be physically secured against tampering

3.6.7 Virtual Private Network (VPN) Devices - Requirements

In some cases, it is necessary for remote devices (e.g. as part of an authorised work-from-home arrangement) to connect remotely to the *GoS* network. Where this is a requirement then VPN connections must conform to the following requirements.

Requirement	Description
In addition to the "All network infrastructure" and "Basic Build" requirements, Virtual Private Network (VPN) must meet the following requirements	VPN devices must be implemented within a dedicated DMZ
	Filtering rules must be implemented to allow VPN users to connect only to systems for which they have a business requirement to access
	Split tunnelling is to be disabled on VPN clients
	Connections are to be authenticated using Extensible Authentication Protocol (EAP), or an industry recognised secure alternative;
	Two-factor authentication must be used for all remote-access VPN connections
	Use of the VPN is to be restricted to those with a valid business reason for use

[14] https://www.arubanetworks.com/assets/wp/WP_GovernmentSecurity.pdf

3.6.8 Using Internet Protocol Version 6 - Requirements

Internet Protocol version 6 (IPv6) functionality can introduce additional risks to a network that must be managed. The requirements below are designed to help manage those risks.

Note: The below table provide a starting point for appropriate configuration requirements for IPv6 implementations. You can access more detailed guides to supplement this standard from a range of resources, based on your organisation's needs. See for example the NIST Special Publication 800-119 providing guidelines for the Secure Deployment of IPv6 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf and a summary of this Special Publication at https://www.nist.gov/publications/internet-protocol-version-6-ipv6-nist-guidelines-help-organizations-manage-secure

Requirement	Description
Internet Protocol v6 (IPv6) implementations within <Company Name> must meet the following requirements	Dual-stack network devices and ICT equipment that support IPv6 must disable the functionality unless it is a documented requirement
	Network security devices on IPv6 or dual-stack networks must be IPv6 capable.
	Unless explicitly required, IPv6 tunnelling must be disabled on all network devices and ICT equipment.
	IPv6 tunnelling must be blocked by network security devices at externally connected network boundaries.
	Dynamically assigned IPv6 addresses should be configured with DHCPv6 in a stateful manner with lease information stored in a centralised logging facility.

3.6.9 Voice Over Internet Protocol (VOIP) - Requirements

VOIP services and devices are subject to the following requirements.

Requirement	Description
Voice over Internet Protocol (VoIP) implementations within <Company Name> must meet the following requirements	External access to the internal user registrar configured in the VOIP system shall be disabled
	All unnecessary functionality is to be disabled
	The VOIP network must be segregated from the internal corporate network through use of a dedicated VLAN separated by a firewall or Layer 3 switch
	VOIP network traffic must be protected from eavesdropping through use of a VPN tunnel S/MIME or TLS in SIP when travelling over open, public networks.

	VOIP network traffic should be protected from eavesdropping through use of a VPN tunnel S/MIME or TLS in SIP when travelling over internal networks.

3.6.10 Virtualisation - Requirements

The use of Virtual Machine (VM) environments (the emulation of a computer system) may be required for some aspects of *GoS operations*. Where they are used, virtualisation hosts and guest machines must be configured and managed as follows.

Requirement	Description
In addition to the "All network infrastructure", "Basic Build" and "Servers" requirements, virtualisation implementations within <Company Name> must meet the following requirements	Virtual machines on a host must be partitioned to limit access to shared resources and prevent denial of service conditions
	The virtualisation hypervisor must be the primary role of the server, with no additional software installed on the base operating system other than security and backup agents
	The virtualisation services are to be protected by a firewall, allowing only authorised access to services
	VM guests installed on the hypervisor host must not be able to access the hypervisor
	Unused virtual hardware on VMs (e.g. USB ports) is to be disabled
	VMs will not directly access a VM data store or repository
	Copy/paste and drag/drop functionality between guest and host are to be disabled
	Access to the hypervisor is to be restricted to the minimum number of administrators required for management of virtual machine instances;
	Inactive VMs are to be minimised and turned off when not in use;
	If specific measures are available at the hypervisor level to protect virtual workloads, they must be enabled. For example, Hyper-V's Shielded VMs and Guarded Fabric
	Virtual machine data stores must be encrypted in accordance with encryption requirements.
	If the hypervisor hosts Tier 0 servers[15] such as Domain Controllers, the hypervisor host itself must be categorised as a Tier 0 server and secured appropriately
	Virtual Switches and Virtual NICs (Network Interface Cards) must be configured to: • Prevent MAC (Media Access Control) spoofing unless required

[15] https://aka.ms/tiermodel

	• Prevent the use of Promiscuous Mode unless required
	Virtual Machine replication traffic between hypervisor hosts must be encrypted
	Diagnostic interfaces such as VMWare's ESXi Shell must only be enabled for the duration of diagnostic work or troubleshooting

4. Definitions

Term	Definition
Vulnerability assessment	Vulnerability assessment involves assessing systems for vulnerabilities in the network services exposed to the GoS environment.
Penetration testing	Like vulnerability testing but attempting manual exploitation of vulnerabilities to provide more accurate reporting of the issues in the systems in scope.
Zone	A segregated network component which comprises of systems with the same risk profile to the organisation.
VLAN	Virtual Local Area Network is the method used in network switches to virtually separate network components.
Proxy Server	A server/device in a computer network that acts as an intermediary for requests from clients seeking resources from other servers.
NTP	Network Time Protocol is used to synchronise time and maintain consistency in time on all network devices and servers in the GoS Environment.
CSP	Cloud Services Provider is the vendor providing services for processing and storing of GoS information off site.
RADIUS	Remote Authentication Dial-In User Service is used to authenticate remote users on network infrastructure devices.
SIEM	Security Information and Event Management system is used as a centralised location where systems send their logs and events being generated on the endpoints to correlate and report on incidents/issues in the GoS environment.
DMZ	De-militarized Zone, is the network segment behind a security enforcement device such as a firewall used to securely host systems that are exposed to the Internet or other untrusted sources.
WAP	Wireless Access Point is a connection point for wireless clients in the GoS environment.
VoIP	Voice over IP is a technology where telephones and management of telephones in a business are managed over a TCP/IP network instead of a traditional physical copper network.

Version Management

Version	Date	Comments and Remarks
1.0		