Norwegian National Security Authority

Guide

Last updated: 2012-09-26

N-03 Security guidance for switches and routers

Guidance on Network Security to comply with the NSM Information Security directive

The N-series of documents produced by NSM specifies requirements and guidance regarding Network Security related issues. Several principles from the G-series *(General IT Security Requirements)* are reused throughout the N-series to clarify how it will affect network related issues. N-01 is the top level document in the N-series.

This guidance, gives generic requirements and recommendations for the functionality of layer 2 (link), and layer 3 (network) in the OSI model, in other words, the traditional switches and routers.

NSM reference: A03 – S:12/00728-1

Norwegian National Security Authority

The Norwegian National Security Authority (NoNSA) is a cross-sectoral professional and supervisory authority within the protective security services in Norway and administers Act of 20 March 1998 relating to Protective Security Services. The purpose of protective security is to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. Protective security measures shall not be more intrusive than strictly necessary, and shall serve to promote a robust and safe society.

Purpose of guides

NSM's guidance activities are intended to build expertise and increase the security level of organisations through increased motivation, ability and willingness to carry out security measures. NSM regularly issues guides to help implement the requirements of the Security Act. NoNSA also publishes guides in other professional areas relating to protective security work.

Postal address
P.O. Box 14
1306 BÆRUM
POSTTERMINAL

Civilian phone/fax
+47 67 86 40 00/+47 67 86 40 09
E-mail address
post@nsm.stat.no

Military phone/fax
515 40 00/515 40 09

URL
www.nsm.stat.no

Content

1 Introduction

1.1 Background

NSM is directed through the Norwegian Security Act § 9 e. to give guidance and advice on, securing information systems that are classified according to the Security Act § 11 and 12.

The N-series of documents produced by NSM specifies requirements and guidance regarding Network Security related issues. It is strongly recommended to read the G-series *(General IT Security Requirements)* prior to this guidance. Several principles from the G-series are reused throughout the N-series to clarify how it will affect network related issues. N-01 is the top level document in the N-series.

This guidance, (N-03) gives generic requirements and recommendations for the functionality of layer 2 (link), and layer 3 (network) in the OSI model, in other words, the traditional switches and routers. These are further referred to as “network devices” in this document. Extending modules and add-ons making network devices multilevel is not covered.

The main requirements are highlighted in yellow boxes. The belonging description to each chapter and requirement is as to be seen as an integrated part of the main requirement.

The requirements in this guidance are written according to RFC 2119. The keywords “must, “must not, “required”, “shall”, “shall not, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC 2119.

This document is a work in progress and will be expanded and updated in later revisions.

NSM encourages readers to provide comments and viewpoints on this document to NSM, post@nsm.stat.no.

1.2 Purpose

Securing network devices and services is a continuous process as for all other security related issues. The intention of the document is to provide guidance for configuring network devices to be less vulnerable. It will not cover all areas, and there exists no such thing as a static secure state in any system or solution. Security is always a continuous process. But by developing carefully considered baselines for security configuration, and continuously improve and implement security functions according to threat and criticality, the risk can be remarkably reduced.

2 Traffic flow and topology

Traffic flows of networks today are often comprehensive. This gives a tremendous challenge in controlling the traffic in a secure manner. But one thing is for sure, to secure traffic flows and reduce possible vulnerabilities, we need a map, an overview, that shows all possible roads, tunnels and ways that traffic can travel.

First of all it is important to define and clarify the purpose and needs for the particular network. What kind of traffic needs to go from one place to another? This information is used to create and maintain filtering mechanisms and check legality of information flows between objects. A map of the expected traffic flow between endpoints is essential groundwork in network design and controlling network traffic. This includes ports, protocols, origins, destinations etc.

a) A flow control policy shall be created[1].

It is also important to map out which ones are your critical services. Where are potential bottlenecks? What services shall cross security zones or boundaries?

The above will eventually generate a suitable network topology. Topology needs to be well documented, and a list of devices created. This goes for **both physical topology and logical design**. Make sure to register any important dependencies. It is also a good idea to group network devices based on their location, mission, criticality and threat level.

b) The network topology shall be documented.

A well structured and organized IP address plan is fundamental for network security. The IP plan and the network design must be closely coherent and well adapted to form and implement network wide IP security policies.

c) A defined and organized IP plan shall be established.

[1] See further description of flow control policy in G-01, chapter 8.6 Controlled Data Flow.

3 Roles and standards

Within network architecture, as for the system platform, there is a need for specifying roles and standards. This will ease the aspect of management, compliance and securing network devices.

Roles
In any network design, disregarding size and complexity, each device, service or function will have an operational purpose, a mission. The assignment could be to switch packets, route traffic, limit access and so on. NSM does not give specific directions for the choice of roles, but they should be logically grouped, a set of functions that relate to each other. Consider carefully issues like location, network-zoning, functionality, criticality, the need for availability, threat level, relations, dependencies etc.

a) Network devices shall be assigned a role.

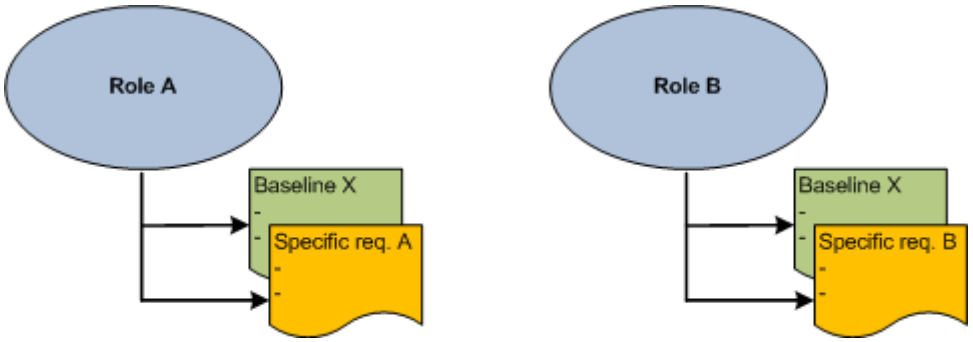
Networks are usually built in some sort of hierarchy. It could, for example, consist of the often used access, distribution and core layer. Most often you will find local switches in the access area connecting end-devices, routers and layer 3 switches in distribution area doing filtering, routing and define multicast domains. In the backbone, or core there might be powerful core switches, and high speed routers. This is one approach to grouping devices.

Baseline
A baseline configuration refers to the creation of a template in order to satisfy the general requirements. This can be a template for both operational and security related configuration of the hardware and software involved. It can be based on product, components, software, versions etc.

b) Each role shall be assigned a baseline configuration, and additional role-specific configuration.

Role-specific requirements
A network device usually forms its role in the design based on the task, and environment it operates in. Similar devices used in environments that require different capabilities, offers additional services, or are exposed to a different threat level, might need additional tailor-made configuration, and in some cases, even a variation of the baseline configuration.

Example



Role A in this generic example has a baseline X, and specific requirements for role A.

Role B has in this example the same baseline X but different specific requirements for role B. But it could also have a different baseline for role B, all depending on how the groupings of roles are done.

4 Products & software

For this section, see also *G-05 Baseline Infosec*.

4.1 Evaluated and certified products

There is a wide range of products, software and versions available. To have some assurance about the quality and standard, especially concerning security related issues, the use of evaluated and certificated products are preferred, and usually required.

Evaluated and certified products shall be used when required.*

**See N-01 Network Security Guidance and G-06 Infosec Assurance for specifications.*

4.2 Operating system

Make sure to choose the newest verified version of the operating system which covers the network wide security and operational requirements. Also be aware of what kind of functionality is installed by default, and what services are enabled by default, because this often varies from one version to another. Do not use early releases.

Use a recent, stable, verified and patched version of the operating system.

This implies that one needs to be updated on potential vulnerabilities for the versions chosen. Make sure all the devices or services defined in the same type of role are standardized*. If, by some reason, there is a need to use a previous version, this shall be well argued, documented, and related security issues carefully considered.

**This does not mean that one cannot use a variation of operating systems in order to ensure security in depth in the network design, but standardize the variations used.*

4.3 Additional software, modules and applications

As for the operating system, use a recent, stable, verified and patched version of all software and additional modules or applications. Be aware that addition of modules and service packs might introduce both vulnerabilities and functionality that can violate the certification.

Use recent, stable, verified and patched versions of additional software.

4.4 Software installation

Software installations on network devices are unfortunately sometimes not always as automated as for more platform related installations. But still, it is just as important to keep in mind;

- The **integrity** of the software
- The **verification** of the software source
- A proper and **secured installation environment** to protect both the devices in question, and the rest of the network.

The same issue arises within the aspect of upgrades. Often improvements and fixes are built into new versions of the software and there might be no option to patch the service in question. The operating system might have to be totally replaced, and there is a risk that such an operation will affect the current configuration.

4.4.1 Installation environment

First time installations shall be done in a protected/isolated environment from a local software repository, and be properly tested before deployment. Later add-ons or upgrades should be centrally distributed protected by a cryptographic mechanism when in transit.

a) Network devices shall be protected during installation.

4.4.2 Installation Source

Make sure the installed software is either from original vendor media, or downloaded from vendor site. Downloads shall be verified on arrival to ensure the integrity of the software.

b) Software from trusted sources shall be installed and integrity verified on arrival.

4.5 Software update/upgrade

Some system upgrades can only be accomplished by replacing the operating system running on the device, and there are not always facilities for patching. To ensure that a new version fully supports the operational needs, it is important to read the release notes carefully before installing.

a) Network devices shall be updated and patched regularly.
b) Integrity of software shall be maintained during system upgrades.

To be able to rollback if something fails, make sure the device has enough memory to keep both the old and the new version stored. Alternatively, replace the device with a spare to perform the upgrade offline without causing a long disruption in network connectivity. In networks with redundant devices, upgrade each redundant device separately and confirm success before upgrading its counterpart.

4.6 Testing and verification

Whether the scenario is first time installation, patching, configuration update or a total upgrade, operational and security functionality must be tested and verified before returning to fully operational use. To assure all necessary areas are covered, a test plan must be established reflecting both operational and security requirements.

a) Operational and security functionality must be tested and verified before placed in operational use.
b) A test plan shall be established.
c) Test results shall be documented.

4.7 Backup and recovery

Prepare for problems in advance. Hardware does fail occasionally, and devices can get compromised. Up to date backups of configuration and installed software images are important. Also, network devices running configuration and start-up configuration must be kept synchronized.

a) A backup routine shall be established.
b) System reboots or power failure shall not affect the configuration.
c) Recovery procedures shall be well documented and tested.

5 General hardening

To make the devices and/or services as robust as possible to withstand an attacker, the devices need to be hardened. This involves limiting access, disabling unnecessary functionality, and securing necessary services in the best way possible. Tightening is an important factor in the creation of secure baseline configurations.

Network devices and services shall be configured according to NSM, and vendors best practice guidelines.

General threats to network devices can include unauthorized access, session hijacking, rerouting, masquerading, Denial of Service, eavesdropping, information theft, to mention some.

5.1 The principle of minimalism

Functionality shall be kept to a minimum.

Try to keep things simple. Too much complexity tends to create security risks. Below are some general advices.

- Make a list of the functions and services that are needed for operational and security reasons. Pinpoint the critical ones.
- Get knowledge of the default settings in the version of the software used. Some versions might have various functionality disabled by default, while others might have the same functions enabled.
- Install only required functionality.
- Disable unused and unnecessary functionality. Services that are not running are not available to be compromised.
- Enable only evaluated and certified functionality. Configure functionality in accordance with the belonging documentation, the TOE (Target of Evaluation), and its PP (Protection Profile).
- Scan the network and specific devices if necessary to verify that unwanted services are not available.
- Secure and limit access to running services.

5.2 Central management

Management of network devices shall be centrally administrated. Network filtering mechanisms must be deployed to prohibit unauthorized administrative access. Management shall be done from a physically or logically separated network. Either way, the purpose is to isolate and protect management traffic from regular user traffic and limit the number of administrative hosts and administrators. Fragmented management might cause reduced situational awareness.

Management of network devices shall be centrally administrated, filtered, isolated and protected.

5.3 QoS

In some cases loss of availability might be as fatal as compromise. A well defined Quality of Service list can assure priority for critical traffic, and reduce the possible impact of flooding.

a) Network devices shall support functionality to handle Quality of Service (QoS) mechanisms.
b) Critical services shall be defined and prioritized.

Traffic should be prioritized and policed as close to the end-point as possible and implemented throughout the network with common policy settings to minimize the impact of priority misuse.

Devices should be able to map COS (Class of Service) values (i.e. VLAN priority) to layer three devices for further processing and network-wide preferences.

5.4 Access control

System-wide authentication, authorization and accounting services (AAA) are required to access network devices remotely. This is to ensure authentication, authorization and accounting. Authenticating is the confirmation of the user and/or device identification before allowing access. Authorizing is to describe user's rights, and accounting is for logging and tracking of user traffic and activity.

a) Network management users shall integrate with the system wide AAA.
b) Re-authentication of devices and users shall occur for proper intervals.

It is also a good idea to bind the AAA service to the loopback interface to be sure the devices are available for management regardless of the status of their interfaces.

5.5 User privileges and passwords

Users on network devices are mainly administrators of some kind, and unauthorized access will often grant the attacker with high privileges and ability to compromise the system. Authenticated access has traditionally not been the main focus in logged activity. A compromised password is often a preferred method for an attacker to explore and compromise systems without causing immediate suspicion.

Requirements for user privileges and password are broadly covered in *G-05 Baseline Infosec Configuration.* Below are some general requirements for user accounts on network devices.

a) Users shall integrate with the system wide AAA.
b) Users shall be assigned individual user accounts.
c) User accounts shall be assigned minimal privileges, and only in accordance with operational needs.
d) The amount of privileged users shall be kept to a minimum.
e) Users must re-authenticate themselves after a period of idle-time.

As indicated by the above requirements, each administrator will need his or her specific username for login to be able to track which user account made changes to configuration.

e) All passwords stored on network devices shall be encrypted.
f) Passwords shall not be sent unencrypted over the network.
g) Password strength shall be according to NSM policy.

Passwords located on the physical network device must be encrypted.

5.6 Default usernames and passwords

Network devices are often pre-configured with a default username and password for administration. If these are not changed, access can be easily retrieved by unauthorized personnel or others.

Default passwords shall be changed.

5.7 Console access

Locally, network devices can be accessed by the physical console port. As for all other user accounts, the console shall be secured by a username and a strong password.

Console access shall be secured by username, password and timeout.

Remember to reserve memory to ensure console access for administration and troubleshooting if the device should run low on memory.

5.8 Loopback interface

The loopback interface can be useful as a standard interface for administration, logging, network time protocol and routing because it will be available even when physical interfaces are down. It will also give one unique source IP per device.

One loopback interface should be defined.

5.9 Unused interfaces

To reduce the risk resulting from unauthorized physical access to network devices, network interfaces that are not strictly needed shall be removed, disabled, or blocked, as appropriate.

Unused network interfaces shall be disabled and blocked.

This also includes unused console, auxiliary ports (AUX) and virtual terminal lines (VTY). The auxiliary port should always be disabled.

5.10 Warning banners

Network banners shall present messages that provide notice of legal rights to users. This is to ensure that unauthorized use of the system and coherent logs can be used as evidence in court. A banner would normally include a statement that only authorized use is allowed and that the device is being monitored. To be sure about the language used, consult with legal staff.

Warning banner shall be deployed on all network devices.

From a security point of view, the banner should not reveal any information about the device or system.

5.11 Unnecessary services

Functionality and services that is not explicit needed is most likely unnecessarily. Network operating systems offer several nice to have services, which also can be nice to have for an intruder. Most of such services can be restricted or disabled.

Disable all unnecessary services on network devices.

Do keep in mind that operating systems for switches not necessarily are identical for routers, and in general for both, some default settings might not appear in a listing of the configuration. Alternatively scan the device to be certain that unwanted services do not run.

Below is a list of typical services to disable:

CDP (Cisco Discovery Protocol)
CDP is proprietary to Cisco and is used to identify devices on a LAN segment. It is considered a security risk both because of the information that it shares and denial of service attacks. If used, it must be disabled on all untrusted interfaces.

LLDP (Link Layer Discovery Protocol)
LLDP is similar to CDP. However, this protocol allows interoperability between other devices that do not support CDP. LLDP can also be used for reconnaissance and network mapping and must be treated in the same manner as CDP. Disable LLDP on all interfaces that connect to untrusted networks.

TCP and UDP small-servers
Small-servers such as echo, discard, daytime and chargen are rarely used, and can be leveraged to launch denial-of-service attacks.

Finger
Finger is a remote user lookup service that shows which users that are logged into a device. It might also reveal running processes. Finger is also vulnerable to denial-of-service attacks.

IP BOOTP server
An IP BOOTP server can distribute system images, and hence be used by a hacker to download the device's software. Disabling this will prohibit the device to act as a BOOTP server.

Identification service
Identd identifies a user's TCP session. It can therefore be used to generate a list of usernames which can be useful for an attacker.

HTTP-/HTTPS server
HTTP is often used for management. The downside is that is sends passwords and content in clear text. If in use, only use HTTPS, force SSL. If not used, disable both.

Remote startup configuration
The service allows a device to load configuration from a remote TFTP-server which uses unsecure transfer file protocols.

TFTP
TFTP allows anyone who can connect to the device to transfer files. If used for first time installation, bind the TFTP client to the loopback interface, and disable when done.

Telnet
Telnet sends information in clear text, and shall be disabled.

Domain name lookup
By default, name requests are often broadcasted. A hacker already monitoring network traffic could be able to record this information. DNS lookups can also cause delay and affect availability if addresses are not resolvable.

SNMP
See chapter 5.14. SNMP should preferably be disabled.

ICMP (Internet Control Message Protocol)
External ICMP connectivity is rarely needed for the proper operation of a network. Through ICMP redirect attacks, a hacker can have packets sent to other devices. Either disable ICMP, or make sure only trusted management areas are able to use it and filter messages by name, type and code. ICMP might be useful in troubleshooting.

DHCP
DHCP (**Dynamic Host Configuration Protocol**) might be an option to run on a router or a L3 switch. Disable if not used.

PAD (Packet Assembler/Disassemble)
This will support X.25 packet assembler. Disable the service if not used.

5.12 TCP Keepalives

This service will send keepalives to idle TCP sessions (inbound and outbound), and is used to ensure that the remote end of the connection is still accessible and half-open or orphaned connections are removed. If the remote side has died, the session will be killed, so it might be a good idea to enable this function.

TCP keepalives should be enabled.

5.13 Time synchronization

Time synchronization is important due to administrative purposes as well as security tracking, incident handling and troubleshooting. Without accurate system clocks, some services might fail. The Network Time Protocol (NTP) is the most common protocol used for this purpose.

a) Device clock time shall be synchronized throughout the system.
b) There shall be at least three trusted clock resources.

Summer time adjustment might create loss of log data or overwriting of log data, so consistency throughout the system is important. The use of UTC is recommended. It is important that clock resources are authenticated and integrity protected. Also consider binding NTP to the loopback interface.

5.14 SNMP

Simple Network Management Protocol (SNMP) is a protocol that is widely used to manage and monitor devices. It also provides information about the health of network devices. It is, however, recommended to disable SNMP.

If you need to use it, use the latest version, and the following needs to be fulfilled:

a) The newest version of SNMP shall be implemented.
b) All SNMP access shall be filtered via ACL's and restricted to management systems or authorized zones.
c) Only read-only access should be allowed.
d) Community strings shall be randomly generated, or at least not easily guessable.
e) Password strength shall be according to NSM policy.
f) SNMP shall authenticate and encrypt packets.

5.15 Access lists

Most routers and switches are capable of performing some sort of packet filtering. Use access lists to restrict access to the device itself. Also, use the flow control policy to create suitable access lists for network traffic in general. In normal scenarios those services that are not explicitly permitted should be prohibited.

ACLs shall be applied to block unauthorized access, block unnecessary traffic, and support the flow control policy.

Packet filters are described in more detail in *N-02 Firewall guidance*.

5.16 Wireless

At the time of writing, no wireless devices have been approved by NSM for encryption or transmission of classified data.

Wireless devices shall be removed or disabled.

Wireless devices include WLAN, Infrared and Bluetooth etc.

5.17 Logging

Software on network devices normally offer detailed debugging for protocols and processes running in the system. Logging and monitoring are used both to reveal health and performance problems, and to discover possible compromises. In order to se correlated relationships, logs shall always be sent to a central log host. Do remember to also secure and harden the log hosts. Log hosts shall be placed in a protected environment.

a) All network devices shall be enabled for logging.
b) Logs shall be sent to dedicated log hosts.

To make traces of network problems or compromise more accurate, include specific timestamps in each log and debug messages.

c) Debug and log messages shall be configured to include timestamps.

Make sure the log level is covering the actual needs and requirements, and also make sure the device can copy and store messages to the internal memory buffer.

d) Buffered logging shall be configured.

Do remember to limit buffer size and history if default is not used.

5.17.1 Health and performance

Performance data is important regarding both system uptime, the integrity of the device and service availability. Examples of performance data could be CPU, memory and buffer utilization. Memory and CPU threshold notifications should alert when configured threshold values are crossed.

e) Events indicating performance problems and functional failures shall be recorded.

Syslog is often used for logging on network devices. Keep in mind that syslog uses UDP and sends information in clear text. Traffic must be protected from regular user traffic, and encrypted if sent outbound.

Syslog offers 8 levels of logging: Emergencies (level 0), alerts (level 1), critical (level 2), errors (level 3) warnings (level 4), notifications (level 5), informational (level 6) and debugging (level 7).
Level 6 shall as a minimum be used to syslog servers. Level 7 is used when needed. Do keep in mind that level 7 might impact device and network stability. However, reduce logging to the console. A high level can overwhelm the console with messages, and the device might become non-responsive. It can be useful, however, to always log at least level 2 for console.

5.17.2 Configuration state and activity

All changes to configuration shall be logged.

This must also include; who made the change, the configuration command entered, and the time that the change was made. The following activity shall be logged:

- System start – and termination
- Account logon and logout
- Login failures
- Changes to local accounts and assigned privileges
- Changes to software and configuration
- Changes in network and interface status
- Network connections / netflow
- Import and export of data to the device
- Filter rules (access denied/drop)

See further requirements for logging in *G-05 Baseline Infosec Configuration*

6 Switch specific

The primary purpose of a switch is to join hosts, servers etc, and create network connectivity between them. It does this on layer 2 (the link layer). A more advanced switch can offer multilevel services, but that is not covered in this guideline.

6.1 Network Access Control

Port based access control (PNAC**)** is used for port based authentication of devices connecting to the network. It provides identification, authentication and authorization of network devices. Unauthorized devices shall be rejected when trying to communicate with the network.

Network device access control shall be enforced at layer 2 (OSI).

6.2 VLAN segmentation

Virtual LANs (IEEE 802.1Q) can be used to segment network groups operating at the same system security level, but with different need to know. VLAN makes it possible for multiple independent logical networks to share the same physical link by grouping subsets of ports into virtual broadcast domains. This gives better control of broadcast, enhances performance and administrative advantages.

Layer 2 devices shall be able to logically segment network groups.

Note that the word *segmentation* is used. VLANs are not an accepted mechanism for separation of networks that are not at the same security level (i.e. classification or authorization level), or system separation.

6.3 Native VLAN

VLAN 1 is the default native VLAN, that is, the untagged VLAN on an 802.1Q trunked switch port. If a switch receives untagged frames on a trunk port, they are assumed to be part of the VLAN that are designated on the switch port as the native VLAN. This is not a preferred situation because it can lead to the crossing of VLAN boundaries. Therefore;

a) VLAN 1 shall not be used.
b) A dedicated native VLAN shall be defined and enforced explicit on each trunk port.
c) All traffic on dedicated native VLANs shall be tagged.

Create unique native VLAN numbers on each trunk. Contact NSM for further information if a certain scenario/situation requires the use of VLAN1.

6.4 Dynamic Trunking Protocol

Cisco's Dynamic Trunking Protocol (DTP) is used for negotiating trunks between VLAN-enabled switches. A trunk port is by default a member of all the VLANs that exist on the switch and carry traffic for all VLANs between the switches. A user facing port shall not be able to auto negotiate a trunk and get unauthorized access to other VLAN's.

a) Dynamic trunking shall be set to off, or no negotiate.
b) Auto trunking shall not be used.

6.5 VLAN Trunking Protocol

The VLAN Trunking Protocol (VTP), also a Cisco proprietary protocol, enables addition, deletion and renaming of VLANs across the network. VLANs are then distributed through all the switches in the domain. To prevent the switch from advertising its VLAN configuration and automatically synchronizing its VLAN database based on advertisements from other switches, VTP needs to be in transparent mode.

Advertised VLAN configuration and automatic synchronisation shall be disabled or ignored.

6.6 DHCP snooping

DHCP (Dynamic Host Configuration Protocol) snooping introduces the concept of trusted and untrusted ports for a DHCP server within a VLAN. DHCP snooping provides DHCP message per-port rate-limiting of DHCP messages, message validation, switch port tracking, as well as protection from DoS (denial-of-service) attacks through the DHCP protocol. If DHCP is used, DHCP snooping shall be used to avoid starvation and spoofing attacks.

DHCP snooping shall be implemented.

6.7 Dynamic ARP Inspection

Dynamic ARP Inspection (DARPII) makes use of the IP and MAC binding table (based on DHCP snooping) to inspect and validate ARP traffic. DARPI can be used to mitigate ARP poisoning attacks on local segments.

Functionality to mitigate ARP poisoning shall be implemented.

6.8 Dynamic Port Access Control Lists

IP Source Guard from Cisco, uses information from DHCP snooping to dynamically configure a port access control list (PACL/PVACL) on the Layer 2 interface, denying any traffic from IP addresses that are not associated in the IP source binding table.

IP Source Guard can be applied to layer 2 interfaces belonging to DHCP snooping-enabled VLAN's and will filter based on IP and MAC addresses. However, this might grow to be a complex structure to manage, and the use of source guard is optional. Although, source guard might be a good solution for smaller networks

The use of dynamic port access control lists is recommended.

6.9 Limiting MAC addresses per port

Cisco's Port Security is used in order to mitigate MAC address spoofing at the access interfaces. Port security makes it possible to limit the number of MAC addresses that can appear on a given port. This will help prevent flooding and DoS attacks against the switch MAC table.

The number of MAC addresses that can appear on an access port should be limited to one.

Port Security can also use dynamically learned (sticky) MAC addresses to ease in the initial configuration. This however, might cause a high level of complexity both in regards of configuration and operational issues.

6.10 Avoiding loops

The spanning tree protocol (STP) is a link layer network protocol for providing loop-free topology for bridged LANs, and avoiding flooding the network. LAN's using this protocol exchange BPDU (Bridge Protocol Data Unit) packets across bridges in order to detect loops. These packets contain information on ports, addresses, priorities and costs. RSTP (Rapid STP) is an evolution of STP and provides a faster convergence after topology change.

Functionality to prevent network loops shall be implemented.

6.10.1 Reduce delay

The listening and learning phase in STP takes quite some time. On access ports it will be preferable to bring the port in immediate forwarding state. Portfast lets the access-port bypass the listening and learning phase when enabled.

Access ports shall be brought in immediate forwarding state..

6.10.2 Block non-authorized bridging devices

BPDU guard prevents the introduction of non-authorized bridging devices when using STP. When detecting bridged software, BPDU guard error-disables the port. BPDU filter prevents sending, receiving and processing BPDUs on a portfast port. Non-authorized bridging devices shall be blocked on access ports.

BPDU guard and BPDU filter shall be enabled on access ports.

6.10.3 Block non-authorized changes in root port and path selection

Root guard prevents switches from transmitting BPDUs that would cause a change in the root port or path selections. Loop guard prevents the alternate root port from being elected unless BPDUs are present.

Root guard and loop guard shall be enabled.

Root Guard is used on designated ports, and does not allow the port to become non-designated, while Loop Guard works on non-designated ports and does not allow the port to become designated.

6.11 Unused switch ports

Unused switch ports shall always be disabled/shutdown and put in an unused VLAN. If not, physical access to a port can potentially give access to a VLAN in used, if configured on the port.

All unused switch ports shall be disabled and put in a dedicated unused VLAN.

7 Router specific

The router's primary purpose is to direct and control data flows across networks. It does this based on packets, addressing and routing tables. A router is usually also able to perform simple traffic filtering by allowing, rejecting or dropping packets. More advanced packet filtering is done by firewalls, firewall modules and application proxies.

7.1 Address filtering

The general advice for filtering traffic on routers is to refer to the flow control policy. Keep strict control of what is considered internal and external networks, and which networks hold higher or lower levels of trust, and make sure traffic is only accepted from the direction and interfaces it is supposed to appear. Deploy coarse-grained or finer-grained filters depending on the role of the device.

In the context of this guidance, ACLs are mostly used to protect and limit access to the network devices themselves. This will typically be filters for remote access, administrative tools and routing protocols.

a) Address filtering shall reflect the flow control policy.
b) Filtering shall be applied to protect the device from unauthorized access. .

Address filtering is covered by *N-02 Firewall Guidance.*

7.2 Broadcasts

There is no reason the router should be able to send traffic to its own interfaces, neither is broadcast needed on a router.

Packet destined to any broadcast address shall be denied.

7.3 IP fragments

Datagram fragmentation makes it possible for a packet with a large PDU (Protocol Data Unit) to be formed to multiple fragments of smaller size than the original, to pass through a smaller MTU (maximum transmission unit) and later be reassembled. This can cause excessive retransmissions when fragments are subject to packet loss, or be used in attacks to evade detection by intrusion detection systems.

IP fragments shall be dropped by ACL's.

7.4 IP options

IP options extend the IP protocol with ability to store protocol-specific states. This type of control traffic was once a good idea for debugging. However, the processing is done in CPU and software, and even a small amount of control traffic packets may bring down a router. Therefore;

Packets containing IP options shall be dropped by ACLs.

7.5 ICMP

Internet Control Message Protocol (ICMP) messages are mainly generated in response to errors. It has a variety of message types, some of which are used for network management, automatically generated and interpreted by devices. This can be quite useful in many situations. However, they can also be handy for an attacker. Therefore some of them should be disabled. Inbound echo, for instance, can be used for denial of service attacks and network reconnaissance.

ICMP messages shall be carefully considered before used.

7.5.1 ICMP unreachable

ICMP unreachable messages are generated by the destination, or its inbound gateway, indicating that the destination is unreachable. These messages can increase CPU utilization on the device and aid in network mapping.

ICMP unreachable should be disabled.

If however used; limit the occurrence by access lists to trusted interfaces.

7.5.2 ICMP redirects

An ICMP redirect message informs a network device of a better path to a destination. It can be generated when a packet is received and transmitted on the same interface. The packet is forwarded and the router sends an ICMP redirect message back. This allows the sender to bypass the router and forward future packets directly to the destination.

ICMP redirects shall be disabled.

A malicious user can exploit the ability of the router to send ICMP redirects by continually sending packets to the router, forcing the router to respond with ICMP redirect messages, resulting in an adverse impact on the CPU and performance of the router.

7.5.3 IP mask reply

An interface's IP address mask will be sent in response to a request. This can be used in network mapping and should be disabled, or restricted to trusted interfaces.

IP mask reply should be disabled.

If used, restrict to trusted interfaces.

7.6 Traceroute

Traceroute is used for printing the IP address of routers that handle a packet as it hops along the network. It deals with ICMP messages such as "Time exceeded" and "unreachable". This can be used by an attacker to create a map of the network.

Inbound traceroute shall be disabled.

7.7 Directed broadcasts

Direct broadcasts allow other devices/hosts to send broadcast across LAN segments. This can be used in several types of attacks. Broadcasts should be kept locally and controlled.

Directed broadcast shall be disabled.

7.8 IP source routing

Source routing allows the sender of a packet to specify the route the packet takes through the network. This will make an attacker able to both discover alternative routes and it might open the possibility to find ways around security controls in the network.

Source routing shall be disabled.

7.9 Unicast reverse-path forwarding

Reverse-path forwarding will verify the source address of IP traffic against routing rules. This reduces the risk of spoofed source addresses, and the possible following denial of service attack.

Reverse-path verification shall be enabled on all interfaces.

7.10 IP proxy ARP

ARP is used to acquire the MAC address of other hosts. Proxy ARP extends a LAN at layer 2 across segments. Proxy ARP can make machines on a subnet reach remote subnets without configuring routing or a default gateway. An attacker can be able to exhaust all available memory by sending a large number of ARP requests. It is also vulnerable to man-in-the-middle attacks.

IP proxy ARP shall be disabled on all interfaces.

7.11 First Hop Redundancy

For devices that act as default gateways, redundancy for gateway failover needs to be in place.

a) A framework between network routers to achieve default gateway failover shall be established.

Examples of First Hop Redundancy Protocols (FHRPs) are Hot Standby Routing Protocol (HSRP) which is a Cisco proprietary protocol, RFC 2281, and Virtual Router Redundancy Protocol (VRRP), RFC 3768.

b) FHRP messages shall be filtered and authenticated.

First Hop Redundancy Protocol messages are exchanged between routers to check the active router condition. These are clear text protocols and therefore vulnerable to DoS attacks, man-in-the-middle attacks and information leakage. Therefore strong authentication and filtering is required.

A strong pre-shared key must be used to authenticate the messages. In addition, filtering VLAN ACLs must be implemented.

7.12 Tunnel interfaces

Tunnelling is usually used to encapsulate and carry a payload over an incompatible network or an insecure public network. Tunnelling will not be discussed further in this document. However;

Tunnel interfaces shall be terminated in their own routing instances and restricted by ACLs.

7.13 Routing and routing protocols

This guide will not cover guidelines and recommendations concerning specific routing protocols. Do consult the vendor documentation on security issues, and use best practice guidelines.

We will however, mention a couple of things to have in mind.

A routers routing table is primarily built by; direct connections, static routing, dynamic routing and default routing. From a security point of view the dynamic routing is of interest, when the router gets update from other routers to create routes. Especially if these protocols are to be used trough firewalls. Whatever routing protocol is used one should always try to think of what might be an intruder's way of getting around, making trouble, compromise etc. For example he or she might try to:

- pick up routing messages/update
- send false routing updates and corrupt tables
- prevent routing updates from being sent or received

The trust of the sender, and the integrity of information, becomes essential. This involves the secrecy - and strength of the authentication key, and also brings up issues as; the number of keys, key lifetime and key management. Either ways, routing information must be isolated from user traffic as for other management traffic.

Annex A Document History

2012-03-19	First internal review (netsik).
2012-05-11	Second internal review.
2012-09-26	First official version