



MindGrove Checklists  
Routers – 10 Important Risks

Revision 2 - January 06

MindGrove Ltd  
 PO Box 729  
 Warrington  
 CHESHIRE  
 WA4 4WZ

Tel: +44 1925 732 757  
 Fax: +44 1925 732 756

Email: [enquiries@mindgrove.co.uk](mailto:enquiries@mindgrove.co.uk)  
 Website: <http://www.mindgrove.co.uk>

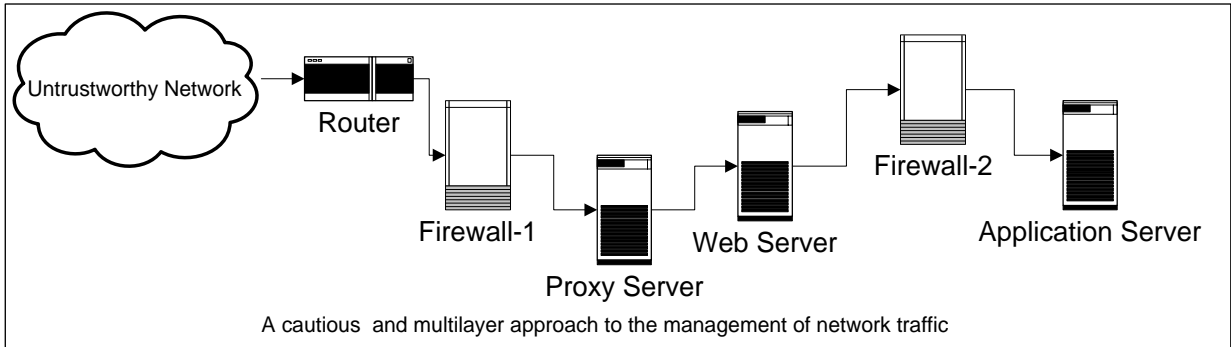
*Note: The MindGrove website has additional useful working and training materials on its resource pages.*

Document			
Document		Template	Size
MindGrove Checklists for Auditors - Routers - 10 important risks		Manual 2005.dot	145920
Status	Final	Version	Format
Issue	1	26	A4
Change History			
Author	Component		Date
MnD	If you find this checklist useful then please tell others about this website and why not send one of your checklists to MindGrove at <a href="mailto:checklists@mindgrove.co.uk">checklists@mindgrove.co.uk</a> and we will publish it for the good of all.		January 06

## Routers – 10 Important Risks ...

Routers are important allies to your proxy servers and firewalls in your multi-layer network security armory.

It's therefore important that you treat them with respect... and configure them correctly!



Use MindGrove's checklist to help make sure you've considered and covered, at least, these 10 major risks.

<p>There may be a risk to the organisation through ...</p>	<p>We will manage this issue by deploying these controls and countermeasures</p>
<p><b>The general control you exercise over routers ...</b></p> <ol style="list-style-type: none"> <li>1. <b>Are you failing</b> to draw up a proper policy for managing and configuring routers...             <ul style="list-style-type: none"> <li>▪ Have you drawn up a router security policy and had it checked by those with subject matter expertise of your vendor (s) router technology?</li> <li>▪ Your policy's been approved, circulated, acknowledged, and accepted by those who deploy, service, configure and maintain your router population?</li> <li>▪ Your policy makes it clear who is authorised to access routers, and who is authorised to configure or maintain them?</li> <li>▪ Your policy makes provision for variable levels of authorisation, and granting of different authorities for the purpose of router maintenance – where the operating system permits it?</li> <li>▪ Your policy takes into account individuals involved in any outsourcing contract you've placed for host or router maintenance?</li> </ul> </li> </ol>	

There may be a risk to the organisation through ...	We will manage this issue by deploying these controls and countermeasures
<ul style="list-style-type: none"> <li>▪ Your policy has made provision for the maintenance of appropriate logs/journals that show who has had access to routers and for what purpose?</li> <li>▪ The logs/journals are made purposeful by routine / periodic / random inspections? The logs are retained for long enough to be useful? See also: 8</li> </ul> <p><b>Planning for router deployments ...</b></p> <p>2. <b>Are you failing</b> to draw up proper plans for deploying routers...</p> <ul style="list-style-type: none"> <li>▪ Is there a formal planning process that defines, scales, deploys and integrates router services into your network services?</li> <li>▪ Have you taken your vendors advice about router management, configuration and security?</li> <li>▪ Are you aware of any internal or external Proof-of-Concept exercises, benchmarking of your suggested architecture (including security features) and the results?</li> <li>▪ Is there an agreed process for deploying new or additional router services whilst minimising disruption to other operational hosts or systems?</li> <li>▪ Is there a process to ensure that all router personnel have proper training (vendor accredited) in management and security disciplines applying to your routers?</li> </ul> <p><b>Base-lining control over routers ...</b></p> <p>3. <b>Are you failing</b> to draw up proper base-lining procedures for configuring routers...</p> <ul style="list-style-type: none"> <li>▪ Your organisation has defined a security architecture in which router services have a known and defined security role; and this in turn is expressed by carefully structured and documented sets of router configuration rules which include access control lists/rules/filter settings?</li> <li>▪ Your organisation has appropriately defined router configuration builds for each security domain?</li> </ul>	

There may be a risk to the organisation through ...	We will manage this issue by deploying these controls and countermeasures
<ul style="list-style-type: none"> <li>▪ There is a complete and current archive of all router configuration builds, these are properly commented for intelligibility and spare copies of these are held in off-site secure storage?</li> <li>▪ There is a process that cross-checks (routine or ad-hoc) masters of router configuration builds against current configurations?</li> <li>▪ Your organisation keeps abreast of security vulnerabilities (notified by vendors, ERTiis and others)?</li> <li>▪ There is an agreed operating system (e.g. CISCO IOS) version and level of patching that forms the baseline software configuration?</li> <li>▪ There is routine security and vulnerability scanning performed, and scanning whenever there is a major configuration change? Different scanners may be used simultaneously to ensure all vulnerabilities are covered?</li> </ul> <p><b>Hardening router security, overall ...</b></p> <p>4. <b>Are you failing</b> to set router hardening standards...</p> <ul style="list-style-type: none"> <li>▪ Have you removed all default router accounts, and removed all default passwords?</li> <li>▪ Are there a minimum number of router accounts and do they have difficult to guess passwords?</li> <li>▪ What about temporary hires or contractors who might help to configure hosts within the system – how will you be able to distinguish them from permanent staff?</li> <li>▪ You have configured master (secret), console, aux and virtual terminal lines with difficult to guess and encrypted (MD5 if possible) passwords? No copies of these passwords or copies of configuration data are available to any unauthorised party?</li> <li>▪ Have you an assurance that the absolute minimum number of TCP/IP Protocols, Services and Ports are permitted by your routing services?</li> </ul>	

There may be a risk to the organisation through ...	We will manage this issue by deploying these controls and countermeasures
<p>In particular you have disabled:</p> <ul style="list-style-type: none"> <li>a) Small services?</li> <li>b) SNMP?</li> <li>c) Remote Configuration – unless bounded by strong authentication?</li> <li>d) Ad-hoc or source routing (loose or tight)?</li> <li>e) HTTP?</li> <li>f) Finger?</li> <li>g) Broadcasts or Multicast Packets?</li> <li>h) BOOTp – on external interfaces?</li> <li>i) ICMP redirects – generally, or, alternatively, you are selectively filtering by ICMP type?</li> </ul> <ul style="list-style-type: none"> <li>▪ You have disabled all but the minimum number of ports necessary to provide a commercial service?</li> <li>▪ Have you an assurance that all the other hosts deployed in the provision of your service are using similarly hardened bare-bones software, to which service packs, patches, corrections and fixes are routinely and obsessively applied?</li> </ul> <p><b>Hardening router security, packet access rules ...</b></p> <p>5. <b>Are you failing</b> to set packet blocking standards...</p> <ul style="list-style-type: none"> <li>▪ All types of access control list have been considered (e.g. CISCO standard, extended and reflexive)?</li> <li>▪ Old packet blocking rule lists are erased prior to entering new packet blocking rule listsiii?</li> </ul> <p>Blocking rules ensure as a minimum...</p> <ul style="list-style-type: none"> <li>▪ Only internal addresses are permitted from internal connections to internal trusted networks, and only external addresses are permitted from external connections?</li> </ul>	

There may be a risk to the organisation through ...	We will manage this issue by deploying these controls and countermeasures
<ul style="list-style-type: none"> <li>▪ Packets are blocked from external networks that are malformed or obviously fake (see RFC 1918; <a href="http://www.rfc-editor.org/rfc.html">http://www.rfc-editor.org/rfc.html</a>)?</li> <li>▪ You are blocking reserved network addresses and loopback addresses (see RFC 1918; <a href="http://www.rfc-editor.org/rfc.html">http://www.rfc-editor.org/rfc.html</a>)?</li> <li>▪ You are selectively filtering ICMP redirects according to type?</li> <li>▪ You are blocking packets from untrusted networks (risk), undesired networks (content), packets which carry the same source and destination address?</li> <li>▪ You are accepting packets (telnet access to the router) from a limited number of trusted addresses? And have explicitly blocked all others?</li> <li>▪ Where you have limited internetworking requirements you have explicitly allowed the required services from the required sources and have explicitly denied all other accesses?</li> </ul> <p><b>Hardening router security, route, route table and host-to-host controls ...</b></p> <p>6. <b>Are you failing</b> to properly set up route and route table controls</p> <ul style="list-style-type: none"> <li>▪ Has the organisation considered the security merits / demerits of static versus dynamic routing tables?</li> <li>▪ Have appropriate controls, authorisation and integrity processes been put in place to ensure that routers cannot be spoofed with fake route updating information?</li> <li>▪ Has the organisation thought through and planned for migration to IPSEC security controls, including host-to-host and tunneling protocols?</li> </ul>	

There may be a risk to the organisation through ...	We will manage this issue by deploying these controls and countermeasures
<p><b>Hardening router security, logging controls ...</b></p> <p>7. <b>Are you failing</b> to properly set up logging and journalisation controls</p> <ul style="list-style-type: none"> <li>▪ Has your organisation implemented router logging so that errors and blocked packets are recorded on a trusted host?</li> <li>▪ Has the organisation configured the logs so that port numbers are recorded?</li> <li>▪ Is the logging host prevented from internal and external intrusions, by appropriate access control, or from becoming the receiver of accidental or malicious log data?</li> <li>▪ Would any individual within the organisation be able to change router configurations and manipulate router logs without collusive activity?</li> <li>▪ Has the organisation properly considered the type and amount of log evidence that you will need to check and keep in order to provide an ability to investigate anomalies, attacks, system errors or to trace the source of system activity?</li> <li>▪ Who is going to examine logs and journals to ensure that activity was as intended?</li> <li>▪ Are the logs set to include date/time information; are the network and all hosts including routers and logging hosts running to the correct time – and is time maintained through an appropriate protocol such as NTP?</li> </ul> <p><b>Communications and Service...</b></p> <p>8. <b>Are you failing</b> to provide for effective MIS reports from the system</p> <ul style="list-style-type: none"> <li>▪ Has your organisation thought about and clearly set down what MIS you are you going to need about whom, why, when and where your staff, temporary staff, contractors and others, deployed and modified router hosts and router configurations?</li> </ul> <p>9. <b>Are you failing</b> to set up a availability service level agreement</p>	

There may be a risk to the organisation through ...	We will manage this issue by deploying these controls and countermeasures
<ul style="list-style-type: none"> <li>▪ Has your organisation set out a clear provision for the definition and measurement of availability and robustness of router based service?</li> <li>▪ Is it obvious who puts things right when they go wrong and how issues will be escalated until they are resolved?</li> <li>▪ Who will handle incidents concerning routers and take responsibility for intrusions into your system?</li> <li>▪ Have you clearly thought through issues concerning Business Continuity, Contingency, Backup and Recovery, and Disaster Preparation connected with the router services that you are hosting?</li> <li>▪ Has your router support team clearly demonstrated their ability to meet your service level, performance and bandwidth, and business continuity requirements?</li> </ul> <p><b>Routers and the Law ...</b></p> <p>10. <b>Are you failing</b> to properly evaluate financial and legal matters</p> <ul style="list-style-type: none"> <li>▪ Does your organisation have controlled processes to deal with router host software licences?</li> <li>▪ Is your organisation responsible for the implementation of any legislative regulations concerning privacy or data protection as a result of International cross-border data routing?</li> </ul>	

If you find this checklist useful then please tell others about this website and why not send one of your checklists to MindGrove at [checklists@mindgrove.co.uk](mailto:checklists@mindgrove.co.uk) and we will publish it for the good of all.

## ENDNOTES

---

- <sup>i</sup> A security domain is defined as an area containing users, data and hosts that are embraced by a common set of security rules.
- <sup>ii</sup> Emergency Response Teams – such as CERT/AUSCERT
- <sup>iii</sup> As access lists are matched linearly until a packet matches a rule, we are here ensuring that no old list elements taint the new rule set or force an ambiguous selection