

Titania's Nipper Technical Specification Document

CONTENTS

- » **General Features List – 2-3**
- » **Report Types – 3**
- » **Compliance Policies – 4**
- » **System Requirements – 4**
- » **Supported Devices – 5**
- » **Contact Details – 5**

Why the world's most secure networks use Titania Nipper

General Feature List

Below is a snap shot of some of the features included in Nipper. All of these come as standard within the product, so there are no hidden costs. If you would like to learn more about a specific feature, or don't see what you're looking for, then please get in contact with one of our team of product experts and they will be happy to help.

Feature	Benefit
Reports are generated in seconds	This means that you can collate data quickly and get results instantly so you can act fast.
Competitive per device pricing model	This means that you can purchase the right size license for your network and grow it with your network.
Detailed reports	You can find vulnerabilities on your network that you didn't know existed and do something about it.
Remediation & mitigation advice	This enables you to understand why a vulnerability is an issue and plan how to fix it.
Pre-defined compliance policies	Using our pre-defined policies you can instantly check your security against industry standards, helping to become compliant and avoid fines and breaches.
No network connection needed & offline activation	By not having to connect to the network you can ensure that the software does not introduce additional security issues and can be used in locked down environments.
Fast installation & multi-device activation The software can be downloaded and installed in minutes on multiple machines.	This is perfect for multi-auditor teams where there are several people using the same license. It is also useful for pen testers who go to multiple sites.
Customizable settings & profiles Using Nipper's setting you can tailor the security auditing report to fit your requirements and save these as profiles. Insert your own customer name, logos and classification.	This means you can produce a report that reflects your security standards. Save time otherwise spent editing the report. You can also edit things like removing sensitive info from the report (such as passwords) to remove security risk.
Audit scheduling	Running reports with Nipper takes seconds, but with audit scheduling it is now completely hassle free. With our simple to use scheduler, you can set configuration reviews to be done while you are away from your desk, on a regular or one off basis. This gives you even more time to spend on getting the issues fixed and less time running reports.
Event logging	Event logging enables you to integrate the finding of Nipper into your Windows logging system or SIEM system. This means that when you run your audits, Nipper will automatically log its findings and any errors into your chosen system, making it even easier to manage along side your other applications.

Feature

Extensive device coverage	Nipper supports over 100 different types of devices, making it the most comprehensive in terms of coverage on the market. This means that it can and is used on some of the most complex networks with ease. From a pen testers point of view it is a great tool to give you information on devices that aren't your speciality, so you can give more coverage and value to your clients.
Easy to understand and use Nipper reports are written in plain English, making them easier to understand. They include graphs and summaries. Help guidance is offered throughout the software to explain terminology and functions.	Easy to understand reports with lots of explanation means that users can operate the software straight away and don't need to waste time contacting us for support. Graphs and summaries mean it is easy to report findings to non-technical managers.

Report Types





Nipper produces accurate and actionable results, designed to make your life easier. Our series of reporting options enable you to quickly produce the results in relation to what is important to you.

- » **Titania's Security Audits** – Perform a "best practice" security audit (combining multiple industry checks). Use the Nipper or CVSS rating systems and mitigation advice to prioritize and plan your fixes. This report is highly customizable in both content and appearance and can help check against industry compliance standards.
- » **Mitigation Classification Report** – This report within the security audit gives additional advice to help plan the fixes on your system. Taking into account penetration testing expertise, it estimates how long each vulnerability might take to fix and then orders the issues in this way.
- » **Configuration Report** – Detailed configuration reporting, including information such as: filtering, routing protocols, administration services & more. This report offers a quick, clear view of your device settings.
- » **Vulnerability Audit** – Audit against global public vulnerability repositories such as the: US Govt NVD (National Vulnerability Database) & the NIST CVE (Common Vulnerability and Exposures) databases. Security issues in the public domain are even easier to exploit, this report helps you quickly find and plug these holes.
- » **Comparison Reporting** – Save previous audit reports using Nipper and reload them at a later date, to produce a report that compares the security status of your device.
- » **Raw Change Tracking** – Upload a previous configuration file and compare it against the current file you are auditing. The report will quickly show you what changes have occurred between the two, so you can see what progress has been made, or potentially identify where an error has occurred.
- » **Filter Complexity** – Nipper will highlight to you where overlapping or contradicting rules exist on your device which clutter up your configuration and cause potential insecurities.




Industry Standards

Our customers use Nipper to quickly gain insight and validation against a range of industry standards. The compliance reports types listed below are the pre-defined policies within the software.

However, customers often use the results from other reporting types (such as the Configuration Report and Titania Security Audit) to help with compliance against other standards such as HIPPA, ISO 27001, Cyber Essentials and more.

	<p>The CIS (Center for Internet Security) benchmark – reports can be run against Cisco ASA & Cisco IOS Devices. These reports have been externally certified by CIS and verified as auditing against their baseline.</p>
	<p>PCI (Payment Card Industry) audits - perform the automatable system checks and support integrating this verified data with non-automatable policy checks. Combine the result from the Security Audit and Configuration Report to gather detailed results which offer advice, verify passes and explain failures, so you can quickly become compliant. Please ask for full documentation regarding how to make the most of Nipper for PCI.</p>
	<p>U.S. Military STIG compliance audit developed in conjunction with DoD IA user groups. Nipper is favored by many government and defense agencies because reports are detailed, verifiable and include remediation in line with STIG baselines. Reports can be generated offline for secure environments and scaled up to audit any number of devices.</p>
	<p>A compliance audit against the SANS policy documents. The SANS institute is a trusted industry body which also trains information security professionals. Their policy is a great compliance benchmark to audit against in order to assess your security level.</p>

System Requirements

OS			
Requirements	Microsoft Windows XP or above (Server 2003 or above) 400MB disk space 2GB memory	GNU/Linux (RHEL, Ubuntu, Fedora, CentOS, openSuSE) 300MB disk space 2GB memory	macOS Sierra or above 500MB disk space 2GB memory

Full List of Support Devices

If you don't see your device listed here, please get in contact with our team and we'd be happy to help.

* = Most Popular



Alteon Switched Firewall (CP)



Arista Routing Switches



Barracuda NetContinuum



Bay Networks Accelar Switches



Blue Coat ProxySG



Brocade BigIron Switch
Brocade FastIron Switch*
Brocade NetIron Switch
Brocade ServerIron
Brocade iCX Switch (IronWare)*



Cisco ASR (IOS XR)
Cisco Aironet (IOS)*
Cisco Aironet Wireless AP (IOS)
Cisco Catalyst Switches (CatOS)
Cisco Catalyst Switches (IOS)*
Cisco Catalyst Switches (NMP)
Cisco CRS (IOS XR)
Cisco Content Services Switches
Cisco IDS/IPS
Cisco Nexus Appliances*
Cisco Routers (IOS)*
Cisco Routers (IOS XE)
Cisco Routers (IOS XR)
Cisco Security Appliance (ASA)*
Cisco ASA Appliance Contexts*
Cisco Security Appliance (FWSM)
Cisco Security Appliance (PIX)
Cisco PIX Appliance Contexts
Cisco Wireless LAN



Check Point IP Firewalls
Check Point Firewall Management*
Check Point Power-1 Firewalls*
Check Point VPN-1 Firewalls*
Check Point Appliance*



CyberGuard Firewalls (SecureOS 6)



Crossbeam Firewalls



Dell PowerConnect J EX-Series
Dell PowerConnect J SRX
Dell PowerConnect Switches
Dell SonicWALL NSA
Dell SonicWALL TZ
Dell SuperMassive



Extreme Alpine (ExtremeWare)
Extreme Alpine (XOS)
Extreme BlackDiamond (XOS)
Extreme Summit (ExtremeWare)
Extreme Summit (XOS)



Forcepoint Sidewinder



F5 BIG-IP



Fortinet Fortigate Firewalls



Microsoft Forefront



Foundry Networks BigIron Switch
Foundry Networks FastIron Switch
Foundry Networks NetIron Switch
Foundry Networks ServerIron*



GTA Firewall Appliances



H3C 3600 Series Switches
H3C 5500 Series Switches



Hewlett Packard Enterprise

HP Routers (ComWare and ProCurve)
HP JetDirect Print Servers
HP Switches (ComWare and ProCurve)



Huawei Quidway Switches (3COM)
Huawei Routers
Huawei CX Series Routers
Huawei Eudemon Series Firewalls
Huawei NE Series Routers



IBM Proventia G Series
IBM Proventia M Series



Juniper E Series Routers
Juniper EX Series Switches
Juniper IDP Devices
Juniper ISG Firewalls
Juniper J Series Routers
Juniper M Series Routers
Juniper MX Series Routers
Juniper NetScreen Firewalls*
Juniper SA SSL VPN (IWE)
Juniper SA SSL VPN (JunOS Pulse)
Juniper SRX Firewalls*
Juniper SSG Firewalls (JunOS)
Juniper SSG Firewalls (ScreenOS)
Juniper T Series Routers



Microsoft Forefront Firewalls



McAfee Enterprise Firewall
McAfee Sidewinder



NETGEAR ProSafe FSM Switches
NETGEAR ProSafe FVS Firewalls



Netfilter IPTables



Nortel Contivity Routers
Nortel Ethernet Routing 8k Switch
Nortel Passport 8k Switches
Nortel Switching Firewalls (CP)
Nortel VPN Routers



Nokia IP Firewalls (Check Point)



Palo Alto Firewalls
Palo Alto Panorama



HP ComWare Routers
HP JetDirect Print Servers
HP ProCurve Switches*



Ruggedcom RuggedSwitch



Secure Computing (SecureOS 6)
Secure Computing (SecureOS 7)



Sophos UTM



SonicWALL Firewall (SonicOS)
SonicWALL NSA (SonicOS Enhanced)
SonicWALL Pro (SonicOS)
SonicWALL Pro (SonicOS Enhanced)
SonicWALL TZ (SonicOS)
SonicWALL TZ (SonicOS Enhanced)



WatchGuard 2 Series Firewalls
WatchGuard 5 Series Firewalls
WatchGuard 8 Series Firewalls
WatchGuard 1050 Firewalls
WatchGuard 2050 Firewalls
WatchGuard XTMv
WatchGuard XTM 1500*
WatchGuard XTM 2520*
WatchGuard XTM 3 Series*
WatchGuard X Core (XTM)*
WatchGuard X Edge (SS)
WatchGuard X Edge (XTM)*
WatchGuard X Peak (XTM)*



3COM 4200 Series Switches
3COM 4400 Series Switches
3COM 4500 Series Switches
3COM 5500 Series Switches
3COM SuperStack 3 Firewalls
3COM TippingPoint IDS/IPS

Contact: enquiries@titania.com | +44 (0)1905 888 785 | www.titania.com