

FIRESECURE



INCAPTION, INC
Networking and Security

Increase the immunity of your firewall

Get your Next-Gen Firewall/UTM device Audited,
Reported and Secured today!



Expert-led Manual Firewall
Auditing (400+ checks)

Bespoke
Audit Report

Consultancy-led
Remediation

A Reality Check

You may have a Next-Gen Firewall/UTM as your first line of defence against the cyber threats. But does it have the required immunity to fight against evolving complex threats to your business? A simple check can surprise you with its outcomes.

Research from Gartner suggests that, by 2020, 99% of firewall breaches will be caused by simple firewall misconfigurations, not flaws. Not just misconfiguration which leads to major security problems, unpatched or poorly maintained security products are also a major threat to the organization.

Decreasing Immunity of your Firewall

Over a period of time, the complexity of your firewall may have increased due to an exponential growth of applications in your network. Today, a single firewall in your organization may be configured with hundreds of objects and rules to define web & application access policies, network access and protection policies, allowed services, routing rules, and more.

Maintaining good firewall configurations is a difficult challenge for even the most experienced network administrator. Even a single firewall misconfiguration can result in a devastating impact on the organization, network availability, or regulatory compliance issue. With the increasing firewall rule base, it is difficult for any IT team to examine firewalls effectively and manage firewalls to ensure that the organization network is protected and in compliance. Your firewall may not be immune to fight against today's evolving complex threats.

Right tools to make your security more immune

While the security products are vital to secure your network and data but these are merely tools. Most SME's do not have the right skill set to ensure that the product implemented is configured and setup to the best of the products abilities and industry practices.

We at Incaption offer you a unique consultancy service offering called "FireSecure" to ensure your Next-Gen Firewall / UTM devices are **Manually Audited (400+ checks), bespoke reported and remediated** by highly skilled network security experts and making sure that security device maintains the highest level of security posture and fully compliant with industries best practices. This is a part of basic network security hygiene exercise for any size and shape of Organisation.



*By 2020, 99% of
firewall breaches
will be caused by
misconfiguration*

Gartner.

FireSecure service follows below process

- ⌋ Pre-Engagement
- ⌋ Audit Schedule
- ⌋ Audit Report
- ⌋ Remediation Consultancy
- ⌋ Implementation Schedule

Audit Schedule

Highly skilled Network Security Experts at Incaption have designed comprehensive auditing process to ensure your security device maintains good security posture and is fully compliant with industry best practices.

Below are the highlights of device auditing process:

▪Expert-led Manual Firewall Auditing (400+ checks)

- Review security configuration which includes:
 - ✓ Device Access Policies
 - ✓ Password Management
 - ✓ Firewall Rules
 - ✓ Content Filters
 - ✓ Anti-Malware / Anti-Spam Policies
 - ✓ Intrusion Prevention Rules
 - ✓ Anti-Spoofing Protection
 - ✓ Web Application Firewall (WAF)
 - ✓ Logging and Reporting
- Compare configurations against industry best practices
- Identify unused rules or redundant firewall policies to simplify security configuration
- Identify policy violations that can lead to security breaches
- Identify gaps in compliance



Audit Report

On successful completion of the auditing process, our SOC team prepare a detailed report to make the customer aware of key findings, the security posture of the device and remediation recommendations.

Audit report would contain following key elements:

▪Executive Summary

- Compliance Highlights
- Firewall's Security Posture

▪Comprehensive information of all non-compliance configuration objects

- Description
- Severity
- Reference information such as Policy Name or Rule-ID



Remediation Consultancy

Remediation is the most critical phase of the FireSecure service as it determines what action to take in response to audit findings.

Incaption offers consultancy-led remediation with below features.

▪ Understand, discuss and prioritize configuration changes

- Our team will help the customer to understand the impact of each suggested configuration change and prioritize them as per compliance requirements

▪ Develop an Implementation Schedule

- We strictly follow ITSM based change management process to ensure

- ✓ Security Performance
- ✓ Minimal downtime
- ✓ Proper rollback strategy
- ✓ Authorization

- All changes would be implemented on predefined schedule to avoid any impact on the network



We work with all major vendors, some of which are:



and more...

Americas

Incaption Inc
200 S Wilcox
St. #403 Castle Rock,
CO 80104
Call 888-660-9908 x111, 303-660-9900 x 111
Email:- Bret Jackson
bjackson@incaption.com



INCAPTION, INC
Networking and Security