Firewall Audit

Approach Document

About Us

3 Offices globally- India, Australia and UK

ISO 27001:2013 Certified

50+ Technology Experts

75+ MSPs Served

15+ Countries

30,000+ Nodes

24x7 Operations

95% - Customer Retention Rate

Why audit Firewalls?

- Enabling MSP’s become MSSP’s
- Regular audits recommended for important & critical customers
- Comprehensive risk assessment to determine security risks, incorrect configuration, risky rules, etc
- The threat landscape is ever changing – Comprehensive 360 audit at regular intervals helps keep the firewall hardened
- Audits ensure there are no miss in configuration – keeping customers safe
- Services available - Detailed audit reports, report review, consulting & remediation

Team behind Firewall audits

- Firewall Audit is performed by highly skilled and certified engineers
- Day in day out interact with MSP/MSSPs on security requirements
- Best of breed security knowledge and best practices from around the globe
- Day to day update on latest threats and how to secure against them
- Consists of professionals with years of experience in CyberSecurity
- Worked with multiple vendor companies

Audit Approach

- **Audit of any firewall brand (e.g. Sophos, Fortigate, pFsense, Sonicwall etc)**
- We use manually handcrafted rules as per the industry best practices
- These rules help you harden the security and eventually comply to the compliances required
- Like your car is checked for various checkpoints, the firewall is checked against 100+ checkpoints
- Use of Automated tools like pingscan, nmap, kali (Will not impact firewall performance during testing)
- Manual checks included in audit

Onboarding

- There are couple of ways to audit a firewall -
  - Send backup
  - Create read-only administrative user (browse only) – **Recommended**

- Infrassist security team to audit the firewall in read-only mode within time window approved

- MSP's responsibility
  - Whitelist Infrassist's IP to enable access
  - Create read only administrative user

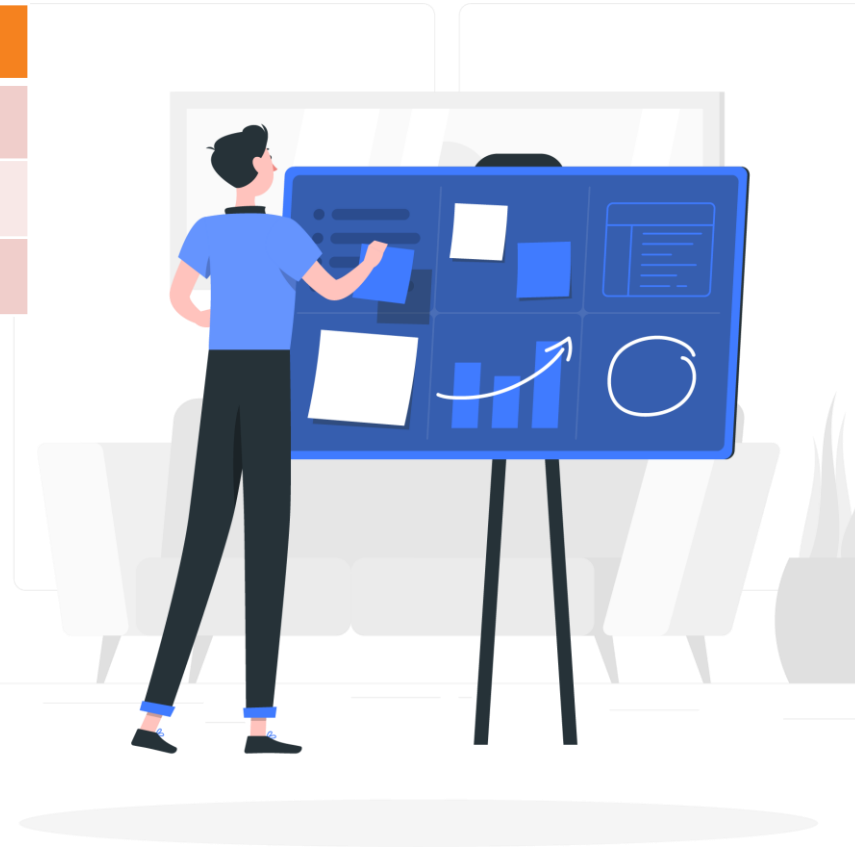
- Infrassist's responsibility
  - Agree on timeline and window to audit (2-3 hours required for the Audit)
  - Present the audit report

Post-Audit

- Post the audit Infrassist team sends a detailed report of findings within 5 working days
- Infrassist team to schedule time with MSP to brief on findings
- Remediation and hardening management performed by Infrassist followed by another audit
- Schedule next Audit

Pricing

Activity	Price/Unit
Audit (Pre/Post) + Report	
Audit (Pre/Post) + Report + Virtual Meeting (Report Review)	
Remediation	T&M



THANK YOU!

INDIA | AUSTRALIA | UK

CONTACT US AT:

Xxx xxx

xxx@infrassist.com

Xxxxx xxxxx