








Firewall Audit Report





Aktiv Software

Firewall Audit Report

 Client Name	Aktiv Software
 Firewall	Sophos
 Start Time	
 Audit Result	Fail
 Risk Meter	High

Firewall Audit Extracts

Security experts at Infrassist have created test cases against which the audit was performed based on years of firewall configuration experience & industry best practices. Below are results of the audit based on severity.

Severity	Pass	Fail	Recommended Config Missing	NA
 High	5	23	3	0
 Medium	2	5	3	3
 Low	0	1	4	0
 Client Dependent	5	20	10	0

Firewall Audit Summary

Recommendations

Our test cases are built around firewall configuration experience and best practices to be followed. Firewall auditors at Infrassist suggest the below recommendations:

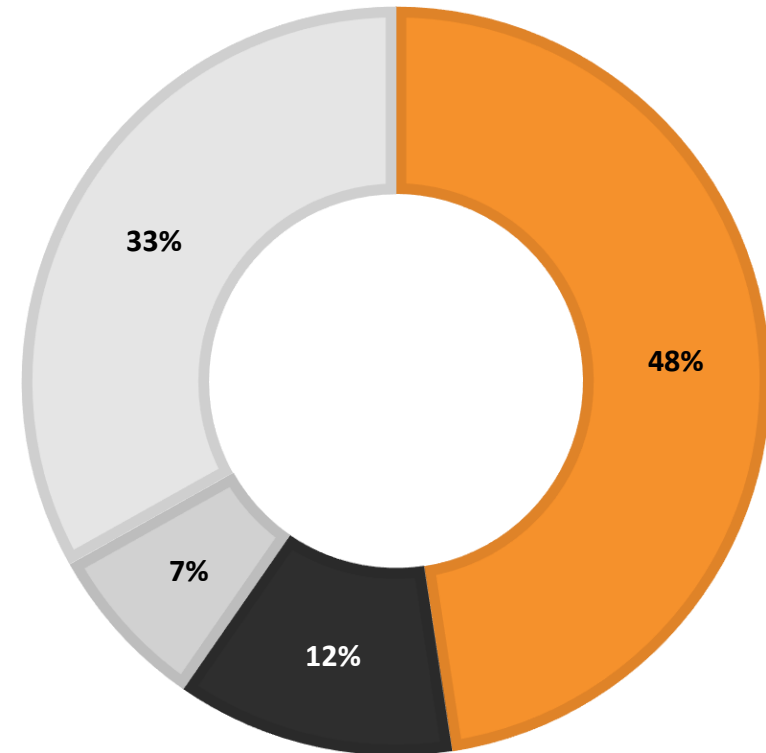
 High Risks

 Medium Risks

 Low Risks

AUDIT DONE AGAINST 82 HANDCRAFTED AUDIT RULES

Applied Rule Not Applied Pass Fail



Fail % 55/82 (67%) | Risk meter – High

There are several items requiring immediate attention and fix, list below

License is expiring is 90 days	Notification email/settings not applied
SSH, Telnet access is enabled for all LAN users	IP/MAC hosts to be defined uniformly using an algorithm
Unused services in LAN are enabled	Unused Firewall rules exists
WAN access is enabled for everyone	Broad firewall rules that allow access to anyone without authentication exist
Unsecure WAN access over HTTP is enabled	No web policies are applied
SSH access is enabled on WAN (Attacks live – screenshot)	No AV scan, SMTP scan are applied
Login security policies can be applied	No IPS policies applied
Password complexity policies missing	Same SSLVPN general user for many users
Last successful backup of the device was in 2017	



Medium Risks

Default global traffic shaping QOS is limited

Custom zones can be made for meaningful firewall rules

Specific country hosts can be created

Login disclaimer can be set





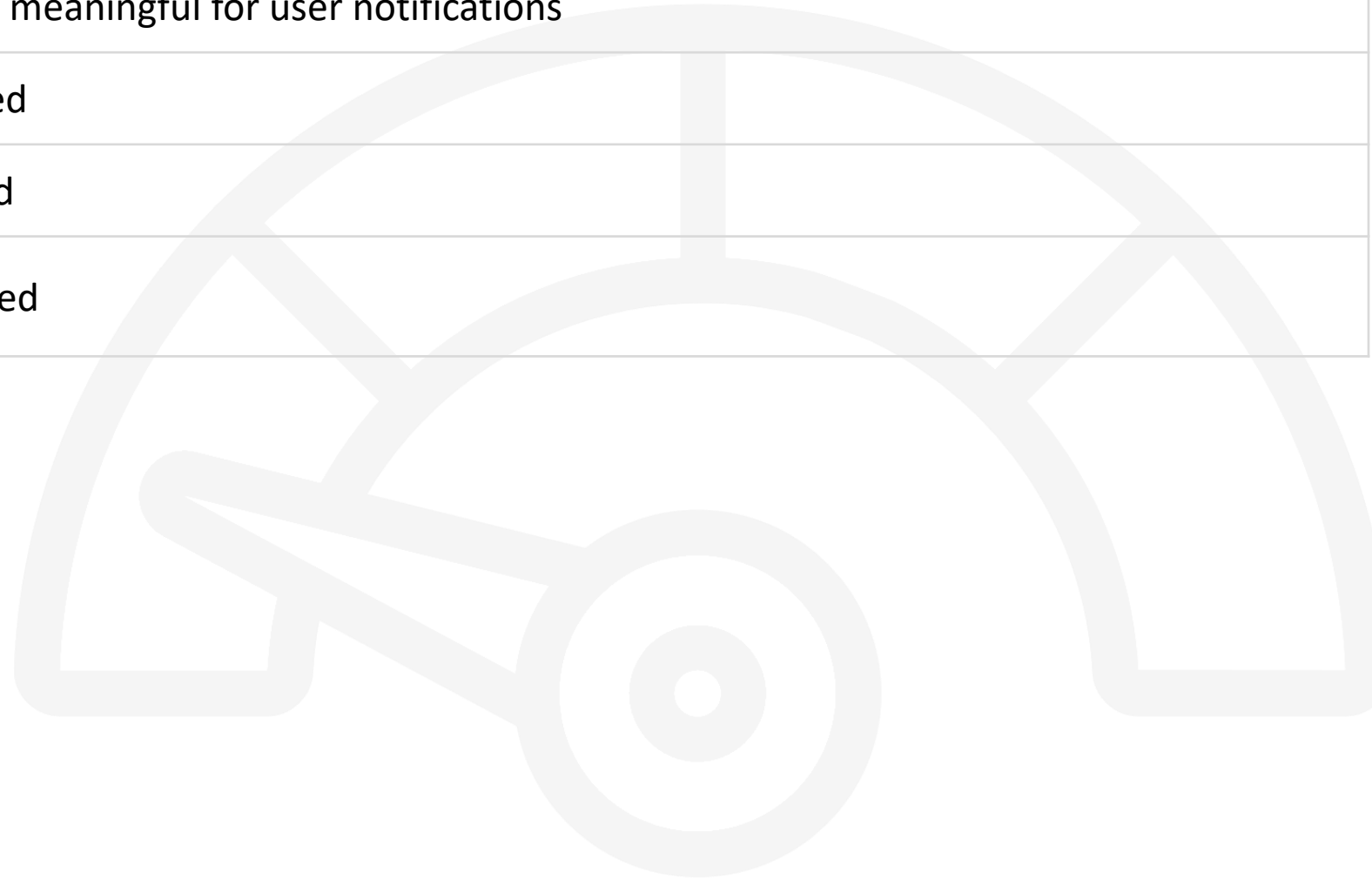
Low Risks

Default system messages can be changed to meaningful for user notifications

Custom time schedule policies can be applied

Custom surfing quota policies can be applied

Custom network quota policies can be applied





Executive Summary

The firewall with AV, antispam, IPS license in place but not being utilized to its full potential. Policies in place will help reduce the attack surface which as of now is very big. It can be reduced with firewall hardening.

Time(approximate) required for a fix: 2 hours

User impact & Change management

- Users will have to login thru the captive portal post firewall hardening
- Admins accessing firewall from outside need to give their IP/FQDN
- Logs and reports schedule to be sent to administrative/management contact for visibility

User impact & Change management

- Bandwidth management will be better than before

Next firewall audit schedule at

DD|MM|YY

THANK YOU!

 INDIA | AUSTRALIA | UK

CONTACT US AT:



XXXXXXXX



xxxxx@infrassist.com



+111111111111111