

PALO ALTO NETWORKS HEALTH CHECK

Optimize the performance of
your Next Generation Firewall

WHY CRITICALSTART?

We're a Palo Alto Networks Certified Professional Services Provider (CPSP) with proven expertise designing, implementing and operating Palo Alto Networks Next Generation security technology.

- 1 Gain immediate insights with little time or effort required on your part.
- 2 Receive a best practices assessment of your configuration and a heat map of your Next Generation Firewall deployment.
- 3 Receive a comprehensive results report, including a prioritized list of action items to correct any observed deficiencies.

Your Next Generation Firewall is a critical component of your security infrastructure and one of your most important cybersecurity investments, so it's important to keep it running in top shape.

CRITICALSTART offers a complimentary Palo Alto Health Check. We analyze the design and configuration for possible security exposures, plus make recommendations to ensure your system is fully optimized and aligned with best practices.



CERTIFIED EXPERTISE

As a Palo Alto Networks Certified Professional Service Provider (CPSP), our team is among an elite group of professionals who possess expertise, tools and ongoing training and resources to enable our customers to maximize their Palo Alto Networks solutions.

HOW IT WORKS

CRITICALSTART will work with you and leverage our tools to collect the necessary technical support and firewall data to perform the Health Check. Once we have reviewed the output, we will generate a short list of prioritized action items. We will then review these with you over a web conference.

CONFIGURATION REVIEW

CRITICALSTART will compare your configuration with current best practices from Palo Alto Networks. We'll also validate the configuration of your Next Generation Firewall feature sets such as: App-ID, User-ID, Content-ID, and Wildfire.

REPORT & REMEDIATE

After our assessment is complete, CRITICALSTART will deliver a post-assessment report. We will share our findings and identify areas that should be addressed. We will also highlight specific opportunities to maximize the effectiveness of your Palo Alto Networks solution and feature sets.

MAXIMIZE THE EFFECTIVENESS OF YOUR NETWORK SECURITY INVESTMENT

Documentation / Help

Metric	2018-04-16 06:30:23	High Technology Average
Total Rule Count	28	
Allow Rule Count	23	
Deny Rule Count	5	
WildFire Adoption %	4.3	39.9
Anti-Spyware Adoption %	4.3	64.9
DNS Sinkhole Adoption %	0.0	36.6
Anti-Virus Adoption %	4.3	64.1
Vulnerability Protection Adoption %	4.3	65.6
URL-Filtering Adoption %	4.3	24.9
Credential Theft Adoption %	0.0	N/A
File-Blocking Adoption %	4.3	22.3
Data-Filtering Adoption %	0.0	12.7
User ID Adoption %	3.6	7.0
App ID Adoption %	78.6	25.1
Service / Port Adoption %	100.0	86.2
Logging Adoption %	96.4	99.1

Monitor Policies 9 Objects 13 Network 24 Device 40 Go to Heatmaps

Zones 10

GlobalProtect

Portals 9

Gateways 2

Network Profiles

IPSec Crypto 3

Zone Protection

Vsys

All Only show records with warnings

gp-gateway vsys: vsys1

Tunnel Mode Enabled True	Ssl Tls Service Profile gp-portal-profile-1	Ssl Tls Service Profile Min Version tls1-2
Certificate Profile None	Tunnel Configuration Enabled False	Tunnel Monitoring Enabled False
Replay Attack Detection Enabled True	Ipssec Crypto Profile default	

Agent Configs

Name	Access Routes
Tunnel All Traffic	None

Best Practice Check Results

- ✗ GP Gateway Agent Config Access Routes (Fail): Please update the following agents so that at a minimum their access routes include "0.0.0.0/0" and "::-0": Tunnel All Traffic
- ✗ GP Gateway Client Authentication (Fail): It is recommended to utilize a Certificate Profile
- ✓ GP Gateway Satellite Tunnel Configuration (Pass)
- ✓ GP Gateway Server Authentication (Pass)
- ✓ GP Gateway Satellite Tunnel Monitoring (Pass)

Notes

- GP Gateway IPSec Crypto Profile: Verify that the IPSec Crypto Profile used (default) meets NIST/EU guidelines

START NOW

Ready for your check up? To learn more about our complimentary Palo Alto Networks Health Check or other ways CRITICALSTART can help you assess and improve your security posture, contact us today at 877.684.2077 or email info@criticalstart.com.