PALO ALTO NETWORKS AND WTI

Out-of-Band Management for Palo Alto Networks NGFW Appliances

Benefits of the Integration

WTI Out-of-Band Rescue integrates with Palo Alto Networks NGFWs to:

- Provide in- and out-of-band CLI access to configuration parameters.
- View console port output during network outages and device failures.
- Log and access console port output using CLI and syslog.
- Securely update DNS settings via in-band and out-of-band connections.

The Challenge

Firewalls need 24/7, year-round uptime to effectively protect networks. When the network is down, troubleshooting sometimes requires personnel to locally access console ports via command line interface (CLI). However, administrators' limited time and resources are not always sufficient during network outages or device failures across large enterprises. So, when trouble tickets and truck rolls must be initiated to visit remote branch offices, downtime and operating costs inevitably increase.

WTI for Out-of-Band Management

WTI designs and manufactures secure, out-of-band management products for local and global networks. Firewalls, routers, and switches must remain in service to support high availability requirements and maintain strict network security standards. Offering a comprehensive strategy, WTI Out-of-Band Rescue™ provides redundant, out-of-band console access and power control to mission-critical infrastructure.

During a network outage caused by internet service provider (ISP) or device failure, WTI utilizes primary, secondary, and tertiary networks to manage power and establish secure console connections to otherwise inaccessible devices.

When deploying WTI devices, administrators can automate power and status alarms for advanced notification before failures occur. In the event of a failure, access to configuration and command parameters can be established quickly and securely to allow for a rapid response, reducing downtime.

Palo Alto Networks

The Palo Alto Networks Security Operating Platform® prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.

Palo Alto Networks and WTI

WTI offers comprehensive out-of-band management of Palo Alto Networks Next-Generation Firewalls when primary network connections become unavailable due to ISP or device failure. During network outages, WTI enables administrators to remotely access configuration settings on Palo Alto Networks Next-Generation Firewalls using validated, secure protocols. This allows troubleshooting of locally and globally deployed devices without initiating truck rolls or compromising your security posture, quickly and securely bringing mission-critical infrastructure and services back online.

WTI increases the visibility of Palo Alto Networks Next-Generation Firewalls console port output across your entire network. Critical data, including configuration parameters and system info, can be captured and saved locally or offsite via syslog for detailed review during network outages. In the event of a severed connection to a remote branch office, WTI can capture and save console port output on Palo Alto Networks Next-Generation Firewalls before primary network access is restored. In addition, WTI allows administrators centralized access to view configuration and system information on multiple devices at branch offices around the globe, simplifying the difficult task of using limited resources to manage a large number of remote locations.

WTI provides secure access to advanced DNS functions when primary and/or secondary ISP connections are switched or disconnected. Through out-of-band connections established by WTI, you can configure primary and secondary DNS server settings—along with other rules and entries—on Palo Alto Networks NGFWs to maximize availability during network outages or ensure seamless transfers between ISPs.

Use Case No. 1

Challenge

Ensure secure access to configuration parameters on Next-Generation Firewalls when primary ISP or network devices fail.

Answer

WTI Out-of-Band Rescue console servers provide secure console port connections via primary and secondary Ethernet as well as tertiary public switched telephone network (PSTN) dial-up.

Benefit

When primary in-band networks fail, administrators can establish secure SSH connections to Next-Generation Firewall console ports via other out-of-band options, delivering access to configuration parameters—such as DNS server settings—used to troubleshoot, secure, and restore network services.

Use Case No. 2

Challenge

Log and securely access console port data across multiple Next-Generation Firewalls

Answer

Up to 40 Next-Generation Firewalls can be connected to buffered serial ports on a single WTI Out-of-Band Rescue device.

Benefit

Console port data from installed Next-Generation Firewalls can be logged and stored locally or sent to syslog servers. Utilizing multiple out-of-band connections, administrators can ensure critical data, such as error messages and audit logs, are saved and accessible to authorized users when the in-band primary network is unavailable.

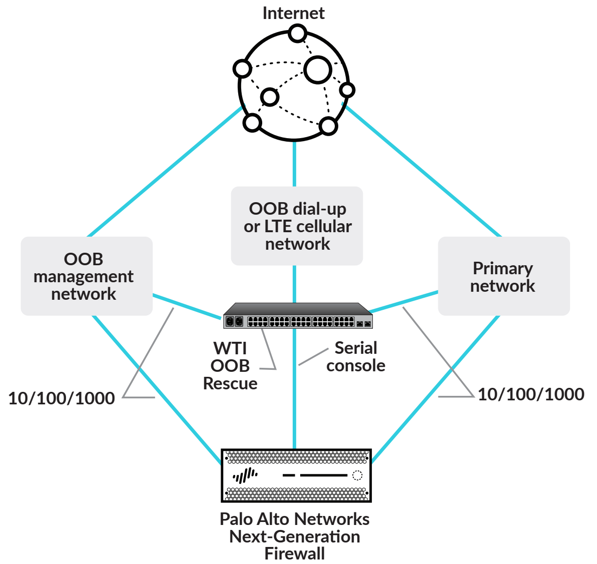

Figure 1: Palo Alto Networks and WTI integration

About WTI

WTI designs and manufactures Secure Out-of-Band Management Solutions for local and globally deployed networks. WTI provides redundant OOB console access and power control to mission critical infrastructure…even when the network is down. WTI products can be purchased factory direct and through various channel partners worldwide. Since 1964, WTI has maintained local in-house manufacturing, engineering & technical support with current headquarters in Irvine, CA. Learn more at www.wti.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com