Salt Typhoon Test Lab

The Salt Typhoon cyberattack against the Unites States has impacted 9 Telecommunications companies (as of May 2025). The attack targets in particular Core Network components such as routing and switching equipment. The impact of the attacks has resulted in the theft of private user information including text messages, IP addresses and phone numbers.

Following the impact of the Salt Typhoon attack on critical telecom infrastructure the FCC has mandated all CSPs are required to secure their networks from unlawful access or interception. CSPs are required to submit an annual certification to the FCC attesting that they have created, updated, and implemented a cybersecurity risk management plan which would strengthen communications from future attacks.

VIAVI can play an important role in the attestation of telecoms infrastructure with TeraVM Security Test. This is a NG Firewall test tool which emulates users and traffic as well as real cybersecurity threats to find the limits of the device under test, the performance of end user traffic while packet inspection takes place and the effectiveness of the firewall in detecting and eliminating unwanted traffic such as CVEs.

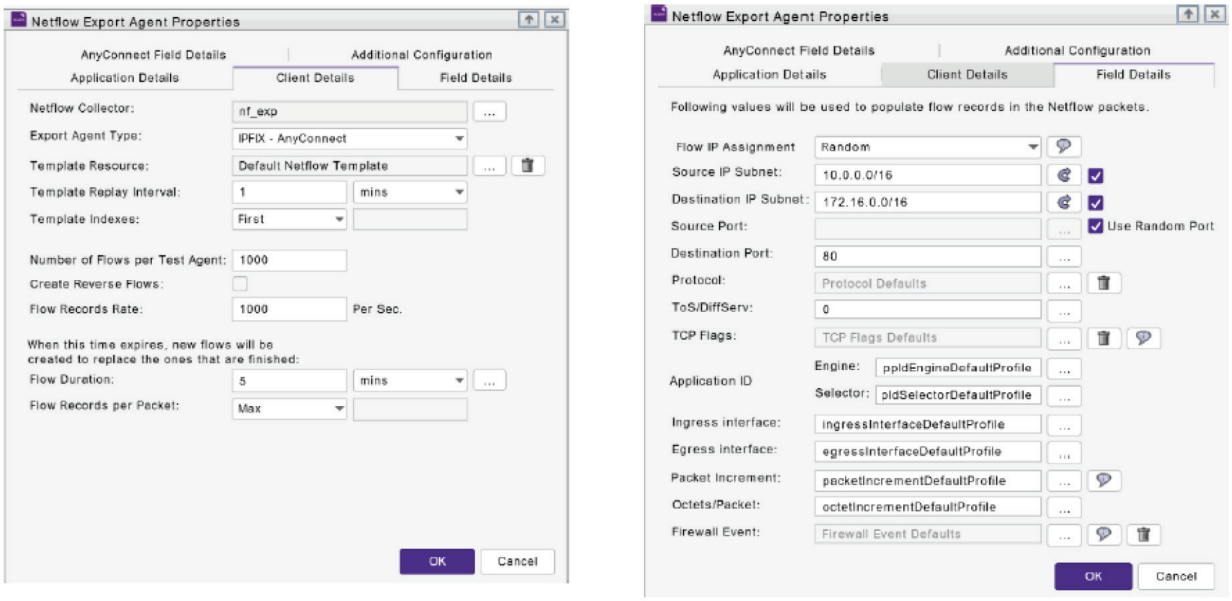
TeraVM Security is a SW only tool which runs on x86 servers or can be cloud hosted. User license can be shared across test labs to maximize utilization. Traffic profiles can be created to any preferred mix e.g., HTTP, TCP, UDP, Voice, Streaming, etc. The cybersecurity database contains over 65,000 threats from industry including the latest Salt Typhoon attacks.

- **Proven:** Established NGFW test tool with over 15 years experience
- **Lightweight VM Deployment:** Runs efficiently on x86 hardware
- **Cloud Compatibility:** Supports GCP, Azure, AWS
- **CyberSecurity Database:** Over 65,000 Industry CVEs supported in regularly updated cybersecurity database
- **Salt Typhoon CVEs:** Latest CVEs from Salt Typhoon attacks added and updated to cybersecurity database
- **Variable Traffic mix:** Create unique traffic mixes of different amounts of different traffic e.g., 20% voice, 30% HTTP, 40% Streaming, etc.
- **Netflow and IPFIX:** Supports network flow monitoring protocols Netflow and IPFIX

Unique Features in TeraVM

Netflow/IPFX emulation in TeraVM

As networks become more complex and demanding organizations need effective test tools to simplify continuous Test (CT). Netflow and IPFIX are network flow monitoring protocols for the collection of network data traffic. These passive monitoring tools allow collections of information to monitor performance without any impact on performance. TeraVM Security test tool emulates Netflow exporter to validate a Netflow Collector – millions of flows can be emulated with user configurable and varying fields. This feature enables emulation of a Netflow record of a Salt Typhoon infected device.



TeraVM supports Netflow protocols v9 and v10 (IPFIX)

CyberSecurity Database

TeraVM Security maintains a database of the latest industry threats and malware. With over 65,000 CVE entries the cybersecurity database entries can be mixed in with good traffic to test the efficiency of the Firewall when it comes to detecting and eliminating threats.

The database is updated bi-weekly with the latest threats.

Vulnerabilities Exploited by Salt Typhoon Attackers

CVE	Description	Availability in VIAVI Cybersecurity Database
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Yes
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Yes
CVE-2023-20198	Cisco IOS XE UI Privilege Escalation Vulnerability	Yes
CVE-2021-26855	Microsoft Exchange Server Server-Side Request Forgery Vulnerability (ProxyLogon)	Yes
CVE-2022-3236	Sophos Firewall Code Injection Vulnerability	Yes
CVE-2023-48788	FortiClient Enterprise Management Server (FortiClientEMS) SQL Injection Vulnerability	Yes
CVE-2024-21887	Ivanti Connect Secure and Ivanti Policy Secure Command Injection Vulnerability	Yes
CVE-2023-46805	Ivanti Connect Secure and Ivanti Policy Secure Authentication Bypass Vulnerability	Yes
CVE-2021-26857	Microsoft Exchange Server Remote Code Execution Vulnerability	Yes
CVE-2021-26858	Microsoft Exchange Server Remote Code Execution Vulnerability	Yes
CVE-2021-27065	Microsoft Exchange Server Remote Code Execution Vulnerability	Yes

Make Contact

For more information, contact sales@viavisolutions.com

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

salttyphoon-testlab-an-wir-nse-ae
30194437 900 0525