Mitel Performance Analytics (MPA) 3.0 (6.4) Security Summary

Introduction

Mitel Performance Analytics (MPA) can be offered to customers in several different deployment architectures. Depending on the architecture, different security principles and tools can be utilized.

On Premise - If a customer chooses to deploy MPA on premise then the MPA server and corresponding modules is subject to the customer's own network security. In this model the MPA server typically sits behind the customers firewall and as such will be governed by that company's security policies. Please see the Mitel Performance Analytics Engineering Guidelines for more details on open port requirements.

On Premise - Air Gapped - Similar to the above, in Air Gapped systems there is no possible connection to external networks, such as the internet, and thus no way to remotely administer the MPA installation. This architecture will also follow the customer's security policies.

Cloud - MPA servers, managed by the Mitel Operations team, hosted in Amazon Web Services in a geographical region close to the customer, have many industry standard security policies and procedures to ensure the application is secure.

Except where otherwise specified, this document will address the Cloud installation option.

Data storage

Mitel Performance Analytics (MPA) is hosted on Amazon Web Services. Mitel uses industry accepted best practices to keep this installation secure. This includes Amazon security groups, firewalled ports, SSH key-based machine logins, and key rotation.

Data access is restricted solely to Mitel employees, all of whom are under strict confidentiality agreements. Only key engineers may access production data, and then only for the purpose of debugging data-related issues as a last resort. In addition, Mitel Support may access your web console to provide guidance as a result of specific incidents or requests.

SNMP Versions

MPA supports the following version of SNMP:

- v1
- v2C
- v3

Audit Log

The audit log file contains records of all actions performed on MPA, when they were performed, who performed them, and where they were performed from. The .csv format audit log can be downloaded for review.

What is logged:

- All device Create, Update, Delete.
- All Remote Access
- Admin User log-in
- User failed login (any)
- MiXML custom command (no details)
- MIB Browser (no details)
- Connectivity Test
- User edited (no details)

What is not logged:

- Non-Admin User log in
- User log out
- Query viewing

Two-Factor Authentication

Two-factor authentication (2FA) provides an extra layer of security for Mitel Performance Analytics beyond your user ID and password. A time-limited passcode generated from another application with no network interaction provides the second factor. This decreases the risk of hackers compromising your Mitel Performance Analytics account.

With 2FA enabled, users must authenticate themselves using a Time-Based One-Time Password algorithm (TOTP) application, in addition to their username and password, before being allowed to login to Mitel Performance Analytics.

Mitel
Powering connections

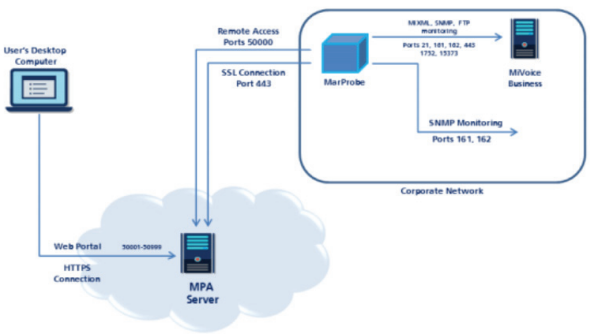
Remote Access Connection Security Features

The Mitel Performance Analytics Remote Access service uses standard IP security mechanisms. The communication links are secured using industry standard encryption and authentication mechanisms.

System Authentication: Mitel Performance Analytics uses a 2048-bit security certificate and authenticates all connection requests.

SSL: All SSL sessions for Mitel Performance Analytics are encrypted and authenticated using RSA-2048 for key exchange and AES 128 for encryption. Cloud installations of MPA use an SSL certificate signed by an industry trusted certificate authority. On-Premise installations of MPA generate a unique self-signed certificate but can be replaced with a customer provided certificate.

SSH: All SSH sessions are encrypted and authenticated using RSA-1024 with rotation for key exchange and AES 128 for encryption. Key Rotation is enabled, generates a new key for each session.



Remote Access Control Settings: Mitel Performance Analytics provides controls for the Remote Access feature through the Probe Settings page. Users can configure the Probe to:

1. Never allow port forwarding, thereby blocking all remote access capabilities
2. Allow port forwarding only to those devices monitored by the Probe
3. Allow port forwarding for all devices on the subnet the Probe is connected to, thereby allow remote access to devices not monitored by the Probe. The Remote Access panel for the Probe provides information on all active remote access sessions.

SOURCE IP ADDRESS RESTRICTION

Mitel Performance Analytics only accepts incoming remote access packets with the source IP address of the user who requested the Remote Access session.

AUDIT LOG REMOTE ACCESS RECORDS

Mitel Performance Analytics maintains an Audit Log for all Remote Access sessions. The Audit Log records the Mitel Performance Analytics user name that initiated the connection, and IP address of the remote device.

USER IP PROTOCOL SECURITY

The link between the user's PC and the Mitel Performance Analytics system uses Internet connectivity for cloud-hosted Mitel Performance Analytics. Therefore, any traffic that is sent over this link is encrypted for security.

SSL/HTTPS is used for all connections to the Mitel Performance Analytics' web portals with security provided by RSA-2048 for key exchange and AES 128 for encryption.

The following table lists commonly used TCP/IP protocols and their encryption levels:

PROTOCOL /PORT	SECURE	APPLICATION
HTTP/80	No	Web
HTTPS/443	Yes	Web
SCP/22	Yes	File Transfer
SFTP/22	Yes	File Transfer
SSH/22	Yes	Secure Session
Telnet/23	No	Terminal Session
FTP/21	No	File Transfer

Mitel cautions against the use of HTTP, Telnet and FTP when using Mitel Performance Analytics Remote Access because the segment of the connection between the user's PC and the Mitel Performance Analytics server is not secured.

AWS Security Practices

Mitel Performance Analytics resides in Amazon Web Services (AWS) and as such is governed by AWS security practices. For more information on AWS see:

- https://aws.amazon.com/security/
- https://d1.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

Mitel
Powering connections

Mitel Internal Security Audits

Mitel has been dedicated to internal security audits and tests since its inception and continues to perform its due diligence in the areas of security vulnerabilities. Mitel regularly performs both Nessus and BURP Scans on its environments and documents the results. If at any time a Mitel partner or customer has questions or concerns regarding the latest test results they simply need to submit a request to support@martellotech.com and a Mitel support representative will be happy to discuss our results with them.

NESSUS SCAN

Nessus allows scans for the following types of vulnerabilities:

1. Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
2. Misconfiguration (e.g. open mail relay, missing patches, etc.).
3. Default passwords, common passwords, and blank or absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch dictionary attacks.
4. Denials of service against the TCP/IP stack by using malformed packets.
5. Preparation for PCI DSS audits.

Mitel performs Nessus scans weekly and the results of these tests may be requested.

BURP SCAN

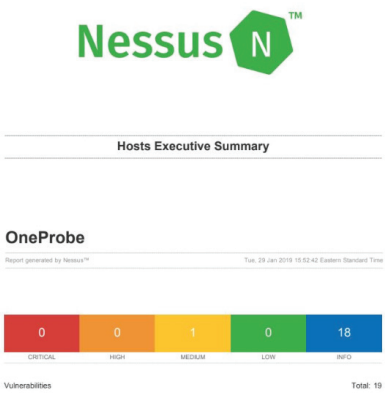
BURP Scan is a graphical tool for testing Web application security. The following components are tested by Mitel on every major software release (minimum 2x per year):

1. HTTP Proxy - It operates as a web proxy server, and sits as a man-in-the-middle between the browser and destination web servers. This allows the interception, inspection and modification of the raw traffic passing in both directions.
2. Scanner - A web application security scanner, used for performing automated vulnerability scans of web applications.
3. Intruder - This tool can perform automated attacks on web applications. The tool offers a configurable algorithm that can generate malicious HTTP requests. The intruder tool can test and detect SQL Injections, Cross-Site Scripting, parameter manipulation and vulnerabilities susceptible to brute-force attacks.
4. Spider - A tool for automatically crawling web applications. It can be used in conjunction with manual mapping techniques to speed up the process of mapping an application's content and functionality.
5. Repeater - A simple tool that can be used to manually test an application. It can be used to modify requests to the server, resend them, and observe the results.
6. Decoder - A tool for transforming encoded data into its canonical form, or for transforming raw data into various encoded and hashed forms. It is capable of intelligently recognizing several encoding formats using heuristic techniques.
7. Comparer - A tool for performing a comparison (a visual "diff") between any two items of data.
8. Extender - Allows the security tester to load BURP extensions, to extend BURP's functionality using the security testers own or third-party code (BAppStore)
9. Sequencer - A tool for analyzing the quality of randomness in a sample of data items. It can be used to test an application's session tokens or other important data items that are intended to be unpredictable, such as anti-CSRF tokens, password reset tokens, etc.

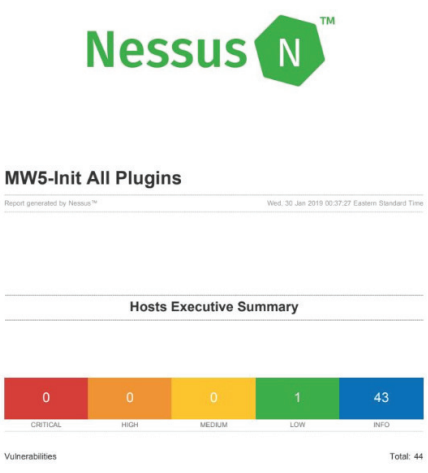
MPA-3.0 GA Scan Results

As previously detailed,internal scans are shown here:

Mitel Probe (Medium is a false positive)



Mitel Instance



Mitel
Powering connections