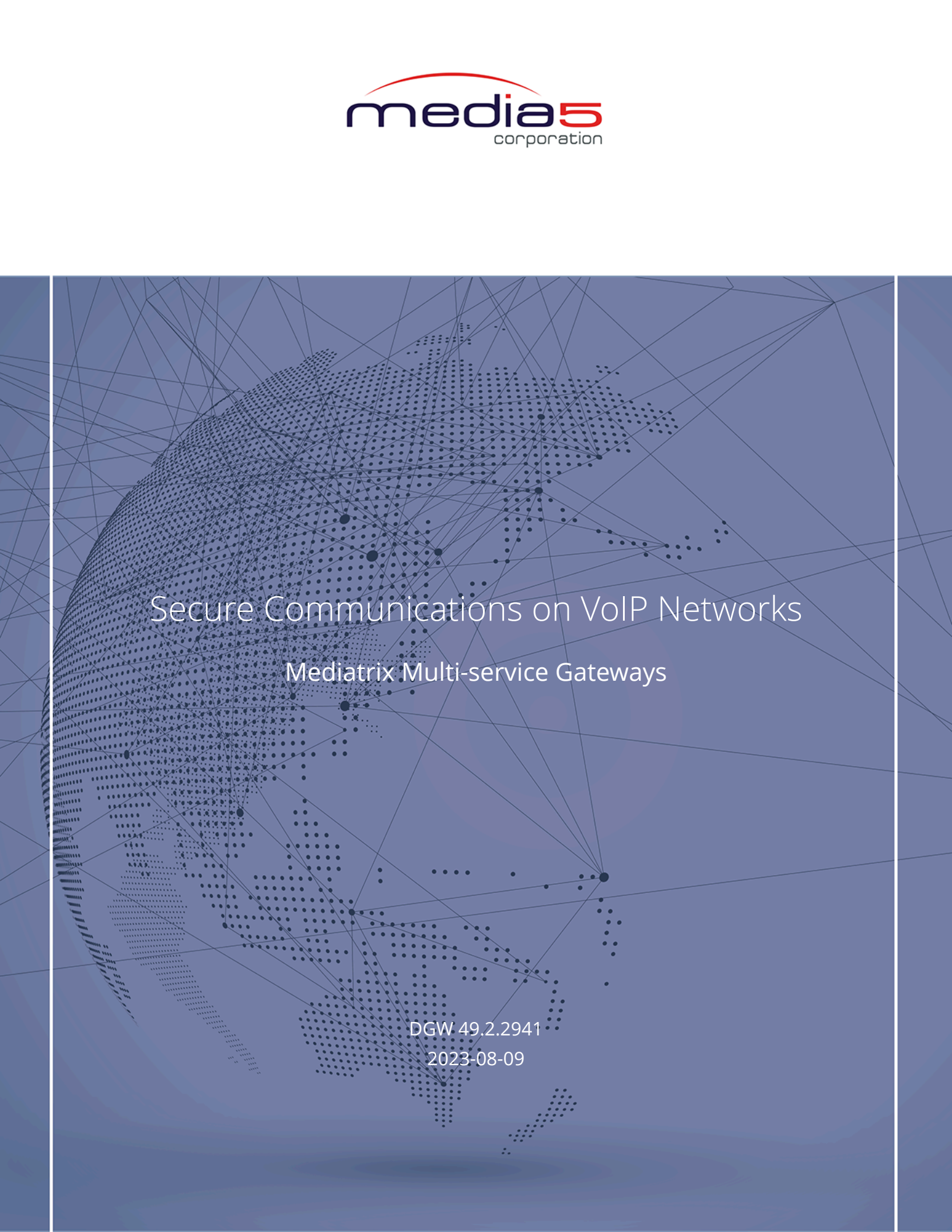


The background of the slide is a dark blue abstract graphic. It features a complex network of thin, light blue lines connecting numerous small, dark blue dots. These dots are arranged in a way that suggests a globe or a map, with the network lines crisscrossing the entire surface. The overall effect is one of a global, interconnected network.

Secure Communications on VoIP Networks

Mediatrix Multi-service Gateways

DGW 49.2.2941

2023-08-09

Table of Contents

Internet Telephony Network Security	4
Authentication	4
X-509 Certificates	4
Transport Layer Security (TLS)	6
Hypertext Transfer Protocol Secure (HTTPS)	6
Communications Security	8
Unit Signaling Security	8
Media Security	9
Denial of Service Attacks	9
Sbc Service	9
Management Security	10
TR-069 Remote Management	12
Password Protection	12
Security Using a Customer Profile	12
Configuration Scripts	13
Command Line Interface (CLI)	13
Simple Network Management Protocol (SNMP)	13
Firewalls	14
Appendix	15
Certificates	15
X-509 Certificates	16
TR-069 or CPE WAN Management Protocol (CWMP)	17

Table of Contents

Transport Layer Security (TLS) Parameters	18
SIP Transport Types	19
Online Help	20
DGW Documentation	21
Copyright Notice	22

Internet Telephony Network Security

At Media5, we use state-of-the-art security technologies to secure our units. Therefore, when using Mediatrix Gateways for Internet telephony network applications, one can be assured to be protected with the best security mechanisms and features available in the industry.

In an Internet telephony network, there are two aspects that must be secured:

- customer communications
- network management

To provide security, the following must be tackled:

- [Signaling security](#)
- [Media security](#)
- [Denial of Service attacks](#)
- [Management Security](#)

Furthermore, several security mechanisms are used in our Mediatrix products to ensure security:

- Data encryption
- [Authentication](#) (p.4)
- [TLS](#) and [HTTPS](#) secured transport protocols
- [Certificates](#)
- [TR-069](#)

Authentication

As defined in the Oxford Dictionary, authentication is the process or action of verifying the identity of a user or process.

In an Internet telephony network environment, authentication will allow the Mediatrix unit to make sure the peer it is communicating with is the proper network or endpoint (unit or end-user device). This provides a level of security for communications as no communication will be allowed if the authentication is not confirmed.

X-509 Certificates

The Mediatrix unit uses digital X-509 certificates which are based on the international X.509 Public Key Infrastructure (PKI) standard. These certificates are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

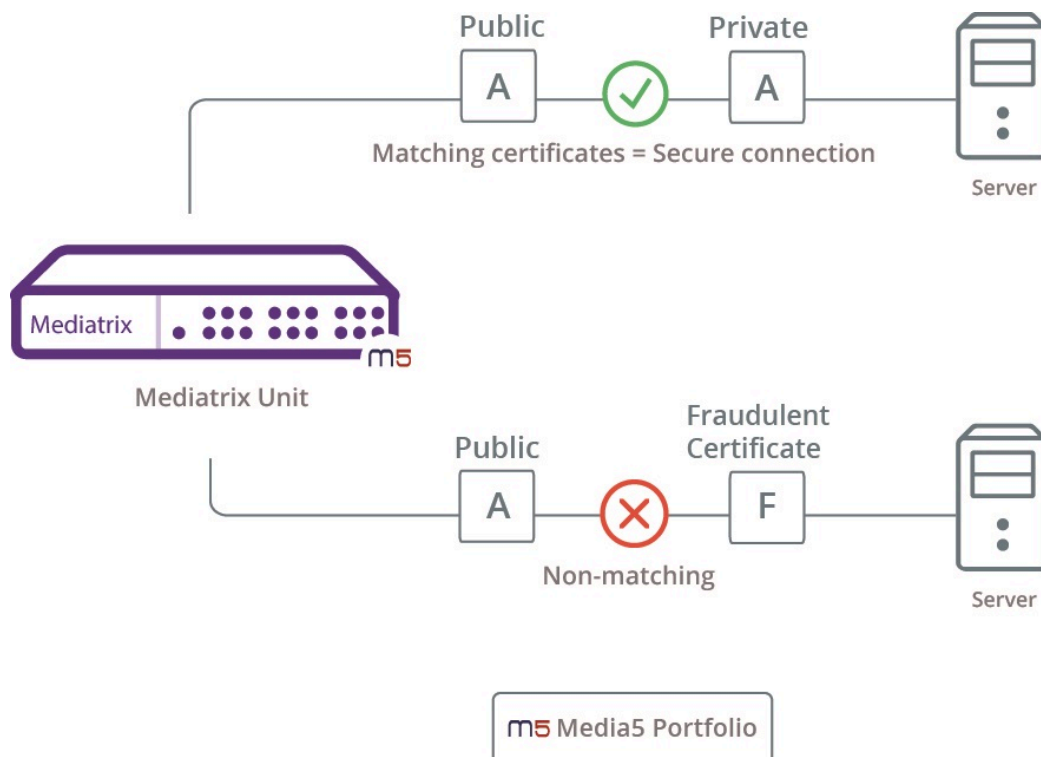
X.509 certificates provide guarantees on confidentiality, authentication, integrity, and non-repudiation. The Public Key Infrastructure (PKI) is a set of rules, specific to an environment, that manages, distributes, stores, and revokes the certificates. Therefore, the PKI guarantees that the signed certificates can be trusted.

Certificates are used to secure the following TLS based connections:

- SIP
- Configuration Web pages
- File transfers (scripts, firmwares, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP-TLS (802.1x)

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates (Client or server)
- whether or not the certificate is delivered by a Certification Authority (CA)



Transport Layer Security (TLS)

The Transport Layer Security protocol provides data privacy and integrity for computer network communications.

In other words, it provides [signaling security](#) and [communication security](#). TLS is a widely used security protocol that allows for:

- Server and Client authentication
- Data confidentiality
- Data integrity

TLS is used for:

- DGW Web Access
- HTTP-based Configuration/Firmware File Transfer
- 802.1X
- SIP communications
- TR-069 (CWMP)

When a [certificate](#) is [authenticated](#), a secure TLS connection is established with a peer. Then [SIP](#), [HTTPS](#), and [TR-069](#) can be used over the TLS connection. TLS connections also prevents man-in-the-middle attacks.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. Once TLS is enabled, it is enabled for all configured SIP gateways.

Although some parameters are available through the Web GUI, many parameters are not accessible through the Web GUI:

- • Cipher Suite
- TLS version
- Certificate validation and trust level

For more details on advanced parameters, refer to [Transport Layer Security \(TLS\) Parameters](#) (p.18).

Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is a transfer protocol widely used to secure communications over Internet telephony networks.

HTTPS allows for communications over Hypertext Transfer Protocol (HTTP) within a connection encrypted by [Transport Layer Security](#) (TLS). HTTPS is mainly used to secure the content of a Web site and securely transfer files.

A communication using HTTPS reasonably guarantees that the targeted peer is the proper one, not an impostor, and that media cannot be read or tampered by any third-party.

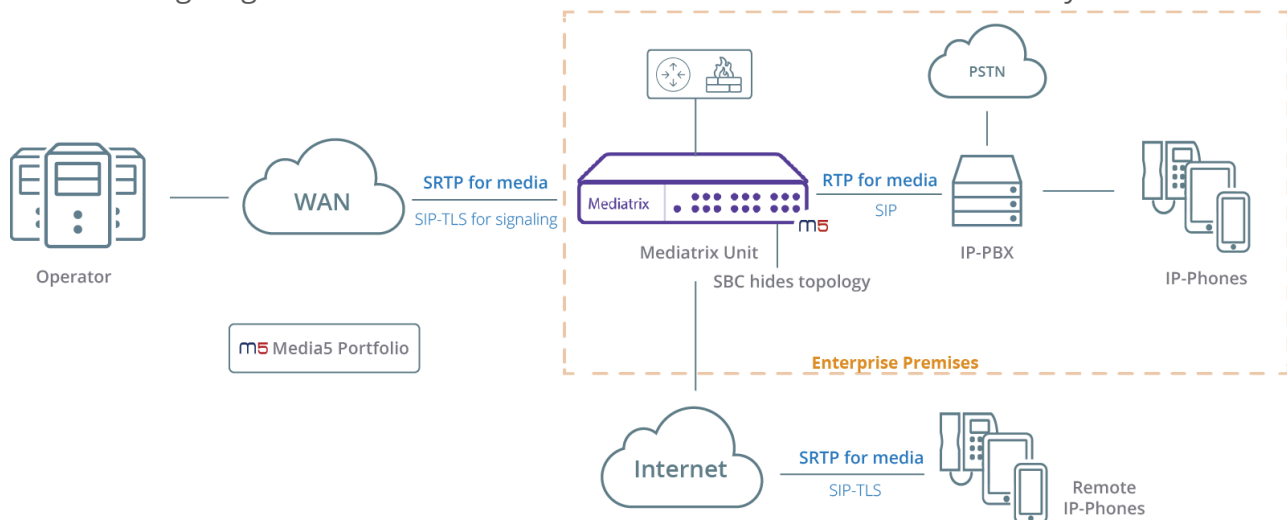
Communications Security

An important aspect of communications security, is that data sent and received from one endpoint to another remains secured, reliable, and private at all times.

When configured for complete security, signaling is performed with TLS with the use of a certificate and the unit transports the audio and video through Secure RTP (SRTP). The Mediatrix unit will make sure that the certificate specifically encrypted for the session and issued by the end user is valid, e.g.:

- the date and hour are not expired
- the certificate was issued by a recognised authority and configured within the unit
- the certificate was issued for the proper IP address or specific FQDN

The following diagram combines several use cases of communications security.



Unit Signaling Security

Signaling is the protocol that activates a device located in the network and establishes calls between peers.

To provide security to signaling, the Mediatrix unit will connect to the network via SIP over TLS. The network is then authenticated by a certificate that guaranties that the Mediatrix unit is connected to a "safe" network.

The network will then authenticate the device with the username and password to make sure the device is part of the network's subscriber list. This authentication is done with the digest authentication. The result of these authentications and verifications provides private and reliable communications between the network and the device. Calls will be established without leaving any possibility to a third party to identify the called or callee number, or to be able to interfere with the communication in any way.

Media Security

Media is voice, video, or data exchanged between 2 endpoints during a communication.

To secure media routed from one endpoint to another, a secret and unique encryption key is generated for that specific exchange of media. For security, the key is exchanged during signaling, via a TLS connection. Once the key is exchanged, endpoints will directly communicate one with another using SRTP with an encrypted communication.

This ensures that voice, video or data, is impossible to decrypt by any one else than the endpoints involved in the communication. Therefore calls will be carried out without leaving any possibility to a third party to eavesdrop the media in any way.

Denial of Service Attacks

The Denial of Service (DoS) attack is an attempt to make a machine or network resource unavailable by overloading it with useless traffic. This has the effect of temporarily or indefinitely interrupting or suspending services of a user connected to the Internet.

The Mediatrix units can address these DoS with the use of [Firewalls](#) and the Sbc service.

Sbc Service

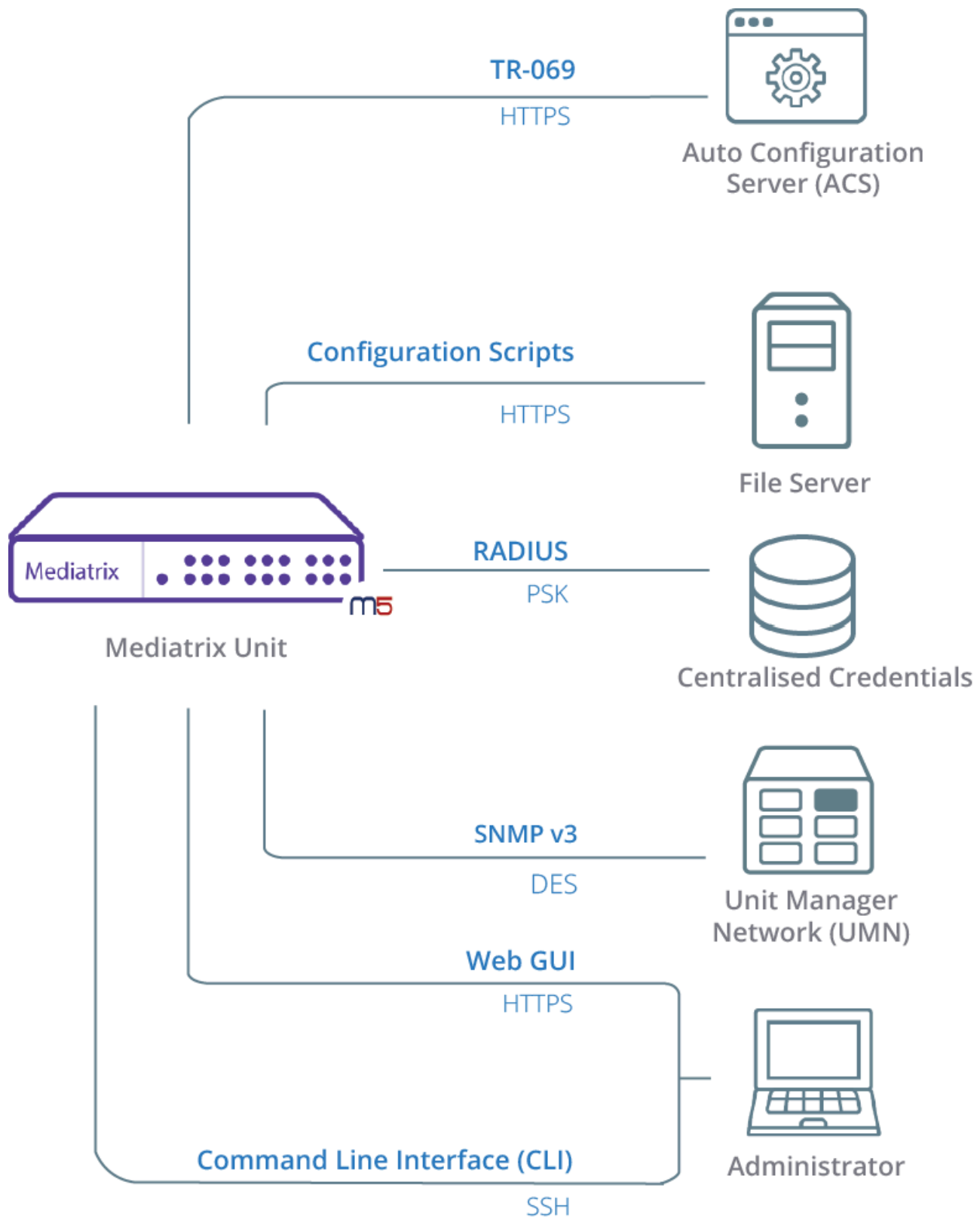
The Sbc service, available only on the Mediatrix Sentinel series, offers major security functionalities.

- set a demarcation point to protect your private network topology information by substituting the IP addresses and the identifiers with aliases.
- secure the communications between the public and the private network by converting signaling between UDP/TCP and [TLS](#).
- secure the media by converting it from RTP to SRTP.
- protect against Denial of Service attacks ([DoS](#)) by automatically blacklisting peers attempting to connect at a frequency higher than normal.

Management Security

An important aspect of Management security is that data used for operation, administration, maintenance, provisioning, and troubleshooting (OAMPT) of the CPE device remains private and secured at all times when management tasks are being carried out.

The Mediatrix units can be configured with different tools, but in all situations, data is always protected; either by using passwords or by Transport Layer Security ([TLS](#)).



TR-069 Remote Management

The TR-069 also known as CWMP, is a Broadband Forum technical specification. This protocol can be used to remotely monitor and update customer-premise equipment configurations and firmware.

Simply said, TR-069 defines a protocol to remotely and automatically configure and manage Mediatrix devices with Auto Configuration Servers (ACS).

Because data used to remotely manage end-user devices include personal and private information (for instance username and passwords) it is vital that the communication channel be secured and the device always be authenticated by the ACS.

Using the HTTPS protocol, the device authenticates the ACS by verifying the ACS certificate and device identity is verified by the ACS using a password which can be changed at each session.

Password Protection

The unit configuration is password-protected.

The unit configuration is restricted in all the interfaces by password protection i.e. a password is required for all security protections (TR-069, SNMPv3, etc.). Local passwords or a centrally managed password (with RADIUS) can be used.

Security Using a Customer Profile

A profile is a factory customisation where parameter values, skins, and branding are defined specifically for a customer.

The customer profile can include security information such as:

- default administrator accounts and [Password Protection](#) policies
- security parameters to be activated
- specific services to activate or not
- [TLS X.509 certificates](#)
- force secure access only (HTTPS and SSH)
- set/disable management options:
 - [SNMP](#) (v1,v2, or v3)
 - [TR-069](#)
 - Provisioning servers
- encrypt configuration scripts for remote management using custom private keys

Configuration Scripts

Carriers and service providers usually define a configuration that will apply to a large number of units in compliance with the network architecture. It is the commands and the parameter values grouped in a text file that produce the Configuration Scripts.

To enforce security, configuration scripts can be encrypted and only Mediatrix units with the matching encryption key will be capable of decrypting and applying the configuration settings. Furthermore, configuration scripts can be downloaded and uploaded using [HTTPS](https://).

Command Line Interface (CLI)

The Command Line Interface (CLI) provides an access to interactively configure all the Mediatrix unit parameters.

IMPORTANT: Although it is possible to configure existing ruleset parameters via the CLI, it is not possible to create or edit a ruleset from the CLI: it must be either imported or directly created or edited in the DGW Web interface.

The CLI is accessed through either a secure SSH session (default) or an unsecure TELNET session. When using a secure SSH session, all communications between Client and server are encrypted before being sent over the network, thus packet sniffers are unable to extract user names, passwords, and other potentially sensitive data. This is the default and recommended way to access the Command Line Interface.

The command interpreter interface of the CLI allows the user to browse the unit parameters, write the command lines, and display the system's notification log.

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) allows you to configure and monitor the device parameters inside a network.

The Mediatrix units support SNMPv3, allowing the authentication and encryption of the management traffic. This feature provides secure connections between Mediatrix devices and Element Management System (EMS). Interoperable, SNMPv3 is a standard-based protocol that is defined in RFCs 3413 to 3415.

Firewalls

Firewalls allows you to create and configure rules to filter packets to ensure the information comes from a trusted sender.

The Mediatrix units support two types of firewalls:

- Local firewalls to filter incoming packets that have the Mediatrix unit as destination
- Network firewalls to filter packets forwarded by the Mediatrix unit used as a router to secure the traffic routed to the devices inside the network.

The local firewall is a security feature that allows you to protect your Mediatrix unit from receiving packets from unwanted or unauthorised peers. The local firewall, by default, drops all incoming packets and lets incoming packets go through only if they match the requirement of a rule.

The network firewall provides a means to dynamically create and configure rules to filter packets forwarded by the unit. Since this is a network firewall, rules only apply to packets forwarded by the unit. The traffic is analysed and filtered by all the rules configured.

Firewalls provides a protection against Denial of Service attacks by limiting the connection frequency under the configurable thresholds and by sending the faulty peers to a blacklist.

Appendix

Certificates

The Mediatrix unit uses digital certificates, which are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates such as:
 - **TlsClient:** The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
 - **TlsServer:** The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.
- whether or not the certificate is owned by a Certification Authority (CA)

Although certificates are factory-installed new ones can also be added. Since TLS certificates are validated in terms of time (certificate validation/expiration date, etc.), the use of NTP (Network Time Protocol) is mandatory when using the security features.

The Mediatrix unit uses two types of certificates:

- **Host Certificates:** used to certify the unit (e.g.: a web server with HTTPS requires a host certificate).
- **Others:** Any other certificate including trusted CA certificates used to certify peers (e.g.: a SIP server with TLS).

The Conf, Cwmp, Eth, Fpu, Nlm, Sbc, and SipEp services are considered secure as they require certificate validation to establish a secure connection to a remote host. The following parameters, available by the CLI, are used to determine whether or not the connection to the remote host should be validated with the service certificate. By default, the parameters are always set to a value requiring validation.

- `Conf.ScriptsTransferCertificateValidation`
- `Cwmp.TransportCertificateValidation`
- `Eth.Eap.CertificateValidation`
- `Fpu.MfpTransferCertificateValidation`
- `Nlm.PCaptureTransferCertificateValidation`

- Sbc.CertificateValidation
- SipEp.InteropTlsCertificateValidation (also available in the DGW Web page under SIP/Interop)

The certificates must be uploaded to the Mediatrix units. They define how a Mediatrix unit will certify the remote host in order to mark it as secure and suitable for a TLS connection. If the Mediatrix unit does not trust the remote certificate (i.e. does not authenticate it with either one of the 3 methods: HostName, trustedCertificate, DnsSrv), then the Mediatrix unit will not establish the connection.

By default it is not possible to upload a Host certificate without first clicking on Activate unsecure certificate transfer. This is because the certificate upload will be done in clear text, which means the private key will be susceptible to interception. Establishing a connection without certificate validation, i.e. establishing an unsecure connection, should only be used :

- for testing purpose,
- if one cannot identify the required CA cert, or
- the CA cert has mismatched Common Name/Subject Alternate Name. (In this case there is no fallback, it will fail if the name does not match)

Certificates are used to secure the following connections:

- SIP
- Configuration Web pages
- File transfers (scripts, firmwares, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP (802.1x)

One common use of the host certificate is to allow HTTPS Web access to the unit (which in this case, the device is the TLS server). For more details refer to the [Technical Bulletins - Creating a Media5 Host Certificate with Open SSL](#) document on the [Media5 Documentation Portal](#).

X-509 Certificates

The Mediatrix unit uses digital X-509 certificates which are based on the international X.509 public key infrastructure (PKI) standard. The certificates are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

X.509 certificates provide guaranties on confidentiality, authentication, integrity, and non-repudiation. It is the Public Key Infrastructure (PKI) which includes hardware, procedures, and software than manages the certificates. The PKI also provides public-key encryption. Therefore, the Public Key Infrastructure provides information that can guaranty that the signed certificates can be trusted.

To enable a TLS connection on Mediatrix units, at least one CA certificate is needed to validate that the certificate presented by the server is valid. This certificate must be uploaded to the Mediatrix units. The Mediatrix unit then checks the server's identity by validating the host name used to contact it against the information found in the server's certificate. If the validation fails, the Mediatrix unit refuses the secure connection. Certificates are used to secure the following connections:

- SIP
- Configuration web pages
- File transfers (scripts, firmwares, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP (802.1x)

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates (TlsClient or TlsServer)
- whether or not the certificate is owned by a Certification Authority (CA)

TR-069 or CPE WAN Management Protocol (CWMP)

The Technical Report 069 (TR-069), also known as CWMP, is a Broadband Forum technical specification. This protocol can be used to monitor and update the Mediatrix unit configurations and firmware. In other words, when using TR-069, the Mediatrix unit can get in contact with an Auto Configuration Server (ACS) to initiate a configuration script transfer/execution and a firmware upgrade.

The first time the Mediatrix unit is connected to the network, it will attempt to contact the Auto Configuration Server (ACS), which is the entry point for the administrator. The Mediatrix unit will obtain the URL of the ACS using either the DHCP server with option 43 or by retrieving the information directly from the Customer's Profile. Therefore, upon start-up, the Mediatrix unit will contact the ACS, which in return will send the required configuration files and initiate, if necessary, a firmware update. This automated sequence is what is referred to as zero-touch, as the Mediatrix unit is automatically configured by the ACS according to the instructions given by the administrator without manual intervention on the unit.

The administrator can determine a schedule for the Mediatrix unit to periodically contact the ACS. These contacts will allow the Mediatrix unit to:

- verify if new configurations are available,
- verify if a new firmware update is available and
- send notifications for monitoring purposes.

Monitoring is achieved by regularly sending notifications to the ACS, through the mean of "Inform" requests, which can be:

- Passive: the information is sent according to the schedule.
- Active: the information is sent immediately when a parameter status changes, regardless of the periodic schedule.

Because the Periodic Informs are initiated by the Mediatrix unit, they have no problem passing through residential or enterprise NAT and firewalls.

Furthermore, the administrator can initiate a connection to the Mediatrix unit to perform immediate maintenance or monitoring. This will only be possible if the NAT firewall has been configured to allow communications initiated by the ACS.

The TR-069 protocol can be activated on units that are already deployed with a licence key (For more details on licences refer to the [Technical Bulletin - How to activate a licence on a Mediatrix unit](#) published on the [Media5 Documentation Portal](#)). However, it can be enabled/disabled for a specific configuration via the Management interface.

TR-069 methods supported by the Mediatrix unit include:

- SetParameterValues
- GetParameterValues
- AddObject
- DeleteObject
- Download
- Reboot
- Upload
- FactoryReset

Transport Layer Security (TLS) Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#). The Reference Guide contains all the parameters used in the DGW software with their description, default values, and interactions.

For certificate transfert

- To set the HTTPS transfer cipher suite for certificate transfer: **Cert.TransferHttpsCipherSuite**
- To set the HTTPS transfer Tls Version for certificate transfer:: **Cert.TransferHttpsTlsVersion**
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

For file transfer

- To set the HTTPS transfer cipher suite for file transfer: **File.TransferHttpsCipherSuite**

- To set the HTTPS transfer Tls Version configuration for file transfer:
File.TransferHttpsTlsVersion

For DGW Web access

- To set the Https Cipher Suite for secure DGW Web access: **Web.HttpsCipherSuite**.
- To set the Http Mode used for DGW Web access: **Web.HttpMode**
- To select the Secure Server Port used to access the DGW Web interface:
Web.SecureServerPort
- To set the HTTPS Cipher Suite for secure DGW Web access: **Web.HttpsCipherSuite**
- To set the Tls Version used for secure DGW Web access: **Web.TlsVersion**

For SIP TLS transport

- To set the TLS transport cipher suite used for secure SIP transport:
SipEp.TransportTlsCipherSuite
- To set Transport Tls Version used for secure SIP transport: **SipEp.TransportTlsVersion**
- To set TLS client authentication: **SipEp.InteropTlsClientAuthenticationEnable**

For TR-069 (CWMP) establishment

- To set the HTTPS transport cipher suite configuration for TR-069 (CWMP):
Cwmp.TransportHttpsCipherSuite
- To set the HTTPS Transport Tls Version configuration for TR-069 (CWMP):
Cwmp.TransportHTTPSTlsVersion
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

SIP Transport Types

You can globally set the transport type for SIP all the endpoints of the Mediatrix unit to either UDP (User Datagram Protocol), TCP (Transmission Control Protocol), or TLS (Transport Layer Security).

Please note that RFC 3261 states the implementations must be able to handle messages up to the maximum datagram packet size. For UDP, this size is 65,535 bytes, including IP and UDP headers. However, the maximum datagram packet size the Mediatrix unit supports for a SIP request or response is 5120 bytes excluding the IP and UDP headers. This should be enough, as a packet is rarely bigger than 2500 bytes.

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the [Media5 Documentation Portal](#).

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes:** Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes:** These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins:** These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide:** They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide:** The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide:** This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com