Securing Communications Between StrongDM Components

Effective Date: June 1, 2023

strongdm

Table of Contents

Background

StrongDM consists of a few core concepts and components required to provide access to virtually any tool or system in your infrastructure. These include the StrongDM Control Plane, and the Customer-operated Data Plane, consisting of Gateways, Relays, and the StrongDM Desktop App. When an access request is made, these components play a key role in determining if access should be granted, provisioning the credentials, and ensuring that the correct level of access is provided.

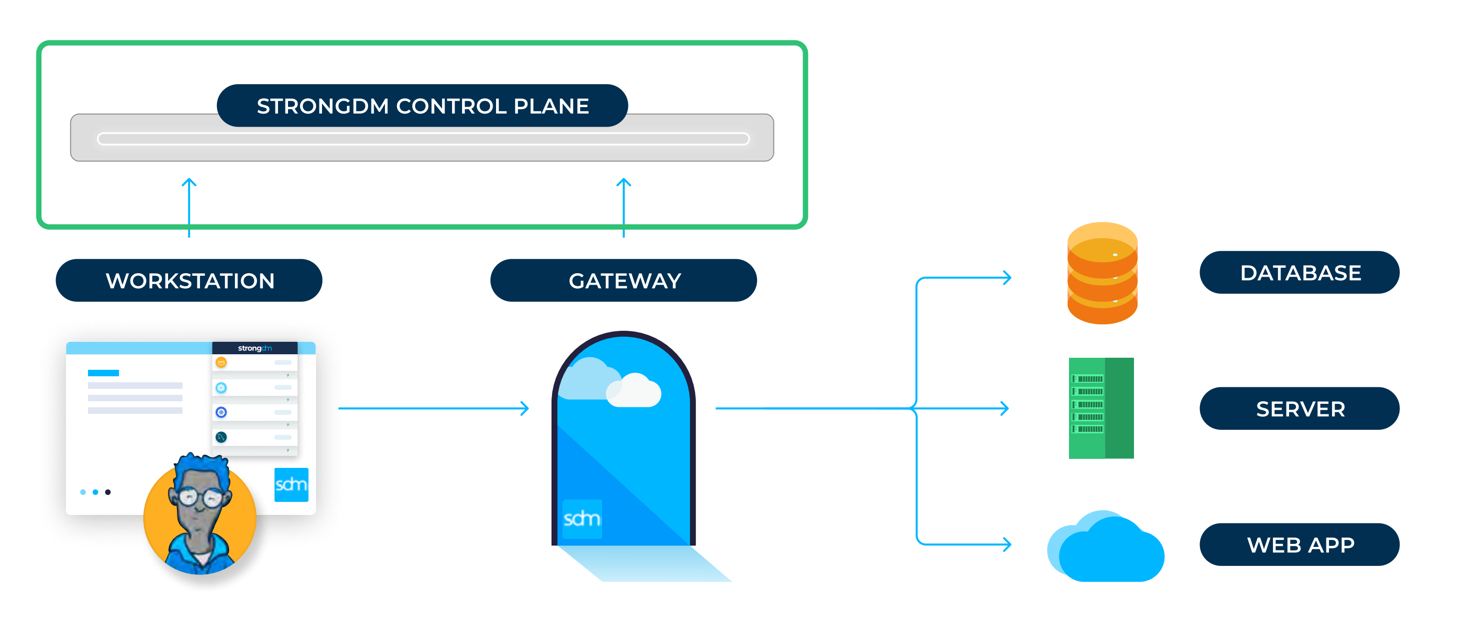
Who Operates What

StrongDM: Control Plane
Customer: Gateways, Relays, Desktop App

StrongDM Platform Architecture

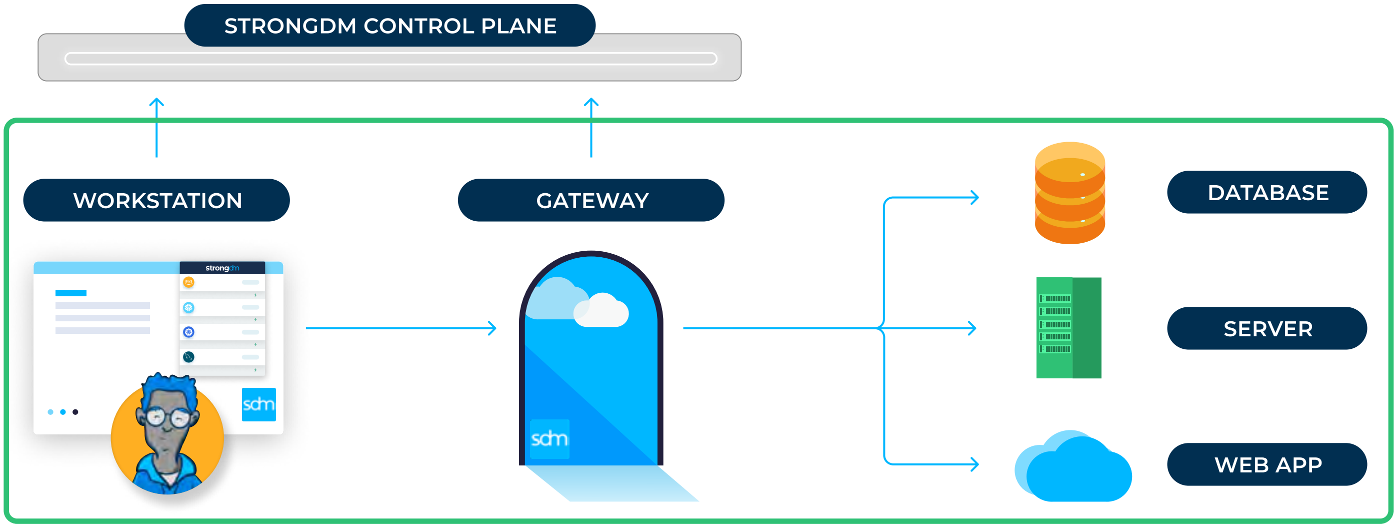
StrongDM-operated Control Plane

The StrongDM Control Plane consists of the Admin UI and access management controls. This is where admins provision and deprovision access, create or change roles, and manage StrongDM system configurations. Furthermore, all StrongDM Gateways and Relays in the Customer's Environment download their configurations from the StrongDM Control Plane.



Customer-operated Data Plane

The Customer-operated Data Plane is the horizontal path between the user, the Gateway, and the network segment to the resources being accessed. This has important security and compliance implications, as any sensitive data being accessed is accessed entirely within the customer's infrastructure.



Components

StrongDM Desktop App (a.k.a. StrongDM Client)

Represented by the "Workstation" above, the StrongDM Desktop App exists on each end user's workstation. The StrongDM Desktop App enables end users to gain access to infrastructure based on their role as defined in the StrongDM Control Plane–this is often known as role-based access control or attribute-based access control (RBAC/ABAC). End users can use either the StrongDM Desktop App or the command line to request access to systems. The Desktop App then tunnels requests from the workstation to a Gateway. Clients are available for macOS, Windows, and Linux, and users can authenticate to the Desktop App via a login or optimally through an identity provider or SSO.

Gateways

Gateways are the entry point to your network. Requests from the StrongDM Desktop App are sent to a Gateway, where the request is decrypted, logged, and conveyed to the database, cluster, web application or server using a StrongDM native protocol for that system. Gateways can be deployed with a DNS entry, and/or sit privately on the corporate network, behind a VPN. Gateways are deployed in pairs and scale horizontally.

Relays

Relays are used in environments that require an egress-only network, such as those that must meet stringent compliance requirements or adhere to security frameworks such as ISO 27xxx. In these situations, Relays, much like Gateways, are how the StrongDM network connects with end resources such as databases and servers.

Unlike Gateways, Relays do not listen for client connections. They're put in place as the last hop to connect directly to the target. When used, a Relay initiates an outbound connection to the Gateway, creating a reverse tunnel into secured networks where inbound traffic is not allowed.

Encryption Basics Within The StrongDM Platform

Libraries and Packages

The StrongDM Platform is written in Go and uses Go's standard library packages to establish and close all TLS sessions. Please refer to the public documentation in the following packages for more information:

- **net**
- **crypto/tls**
- **crypto/x509**

Supported Protocols

As of the time this paper was published, the StrongDM Platform supports only **TLS version 1.2** for any connection between a StrongDM Client and a StrongDM Gateway, or between either of those components and the StrongDM Platform Control Plane.

Supported Ciphers

This will differ depending on what version of StrongDM you are using, and is subject to differ in the future if certain feature flags are present for your organization. At the time this paper was published, the current versions (38.40.1) of the StrongDM Gateways and Agents are configured to use the following ciphers when establishing connections:

For key agreement and exchange, StrongDM uses Elliptic-curve cryptography, and supports the following curves:

```
tlsConfig.CurvePreferences = []tls.CurveID{
    tls.CurveP256,
    tls.X25519,
}
```

For data encryption, StrongDM uses symmetric encryption and supports the following cipher suites:

```
tlsConfig.CipherSuites = []uint16{
    tls.TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
    tls.TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
    tls.TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,
    tls.TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,
    tls.TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
    tls.TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
}
```

Encrypting Data Between Components

Understanding Sessions

A Session is one connection between the StrongDM Desktop App and the StrongDM Gateway. If a User connects to multiple resources that are available to them, then each connection will have its own Session. A Session is established when one executes sdm connect or clicks on the lightning bolt in the Desktop App.

A Session persists, usually, until the user calls sdm disconnect. The session will automatically recreate itself in most scenarios if it is otherwise terminated. These sessions are tied to authentications, so separate logins on separate machines will not have the same set of active sessions.

How Sessions are Established

When a session is established by the StrongDM Client (Desktop App), a number of things happen. First, the StrongDM Client will reach out to the StrongDM Control Plane in order to retrieve appropriate expected certificates in use by other entities in the network. Using the retrieved certificates, the Desktop App will then attempt to initiate a connection with the target Gateway. Should the certificate presented by the Gateway not match the certificate retrieved from the Control Plane, the connection attempt is terminated. The Gateway will also perform the same certificate validation of the Client by reaching out to the Control Plane, requesting and downloading the certificate that it should see presented by the Client, and comparing them. If the presented Client certificate does not match the expected certificate, the connection is terminated.

Assuming that the certificate validation passes in both directions, the Client and Gateway negotiate and establish a TLS v1.2 encrypted connection using the standard libraries and ciphers detailed above. In addition to verified TLS, individual requests to establish long lived Links between entities in this network will have signatures created and verified incorporating the request timestamp, StrongDM vertical, method, and request payload being executed as additional protection against replay attacks or MITM attacks.

Links between entities in this network will have signatures created and verified incorporating the request timestamp, StrongDM vertical, method, and request payload being executed as additional protection against replay attacks or MITM attacks.

How Sessions are Maintained

Sessions in use are actively polled by both servers and nodes enforcing that the sessions heartbeat and that users accessing resources do not lose access to said resources; if they do, broadcasts are delivered to all entities in the network requesting the session be closed; if these broadcasts fail, regular polling attempts to verify connections will also return back to Gateways and Relays that those sessions should be closed. If that fails because a Node is blocked from communicating with the Control Plane, the Control Plane will notice the node refusing to send heartbeats after 60 seconds, and requests will be rerouted to nodes that are heartbeating.

strongdm

StrongDM is a Dynamic Access Management platform that puts people first by giving technical staff a direct route to the critical infrastructure they need to be their most productive. End users enjoy fast, intuitive, and auditable access to the resources they need. Administrators gain precise controls, eliminating unauthorized and excessive access permissions. IT, Security, DevOps, and Compliance teams can easily answer who did what, where, and when with comprehensive audit logs. It seamlessly and securely integrates with every environment and protocol your team needs, with responsive 24/7 support.