HP Anyware Deployment scenarios   **Appendix 1**

Overview

Cloud Access Software enables PCoIP connections between users and remote workstations or desktops using any of several connection models dependent on number of users, location of users relative to remote workstations, your desire to incorporate public cloud workstations and your authentication requirements. Ultimately, your deployment architecture may be based on one or more of these connection models according to your corporate use case:

- Unmanaged direct connection

Solutions for Managed Connections with CAS Manager

- Managed connections for on-site users

- Managed connections for WAN users connecting to on-premises resources

- Managed connections for on-site users and public cloud workstations

- Managed connections for remote workstations in multicloud environments

- Work-from-Home Options with Cloud Access Software

You can choose to license your Cloud Access Software deployment using the Teradici Cloud Licensing Service or a PCoIP License Server, as described here.

Unmanaged Direct Connections

Unmanaged direct connections as shown below are well suited to proof of concepts, trials and small to medium sized LAN deployments where flexibility in machine assignment and multifactor authentication may not be required. Each PCoIP endpoint connects directly to the IP address of a remote workstation.
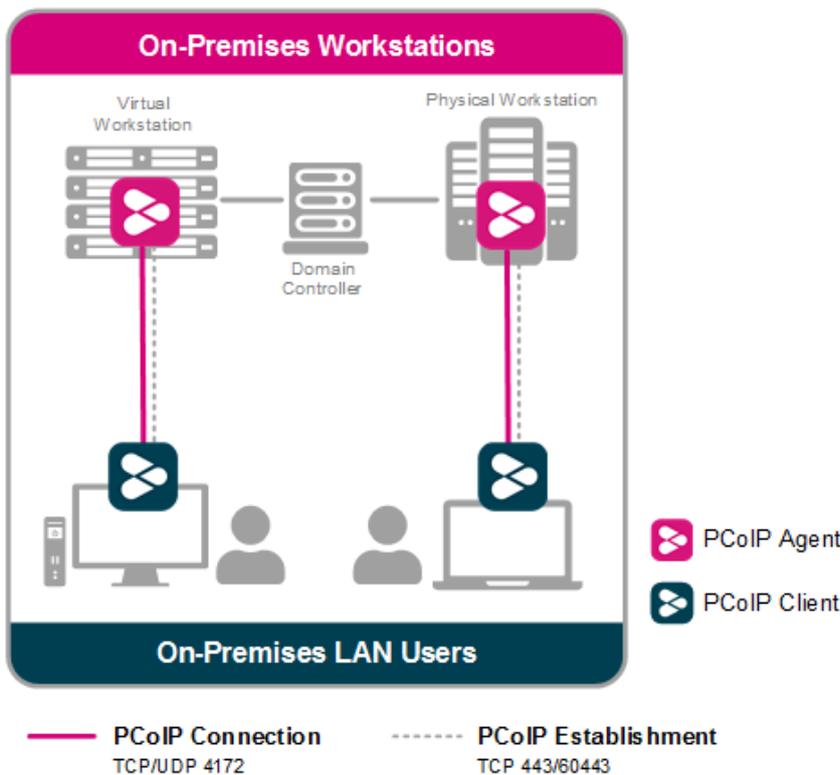
Each PCoIP Client connects to PCoIP Agent software installed on a remote workstation. To learn more about PCoIP Clients, see PCoIP Clients. To learn more about PCoIP Agents, see PCoIP Agents.

Solutions for Managed Connections with CAS Manager

CAS Manager is a Teradici management plane enabling users to configure, manage and monitor brokering of remote workstations. CAS Manager enables highly-scalable and cost-effective Cloud Access Software deployments by managing cloud compute costs by brokering PCoIP connections to remote Windows or Linux workstations.

CAS Manager is offered in 2 variants – as a Teradici managed Service, and as an installable instance deployed and managed by corporate IT in their on-premises or cloud environments. For information on CAS Manager as a Service, see here.

CAS Manager also requires an external component called a CAS Connector that resides in the corporate deployment. CAS Connector is an access hub that facilitates PCoIP connections to remote desktops and workstations by providing user authentication, entitlement and security gateway services. For more information on CAS Connector, see the Key Concepts section in the CAS Manager as a Service guide.

CAS Manager enables you to install multiple CAS Connectors in multiple cloud regions as well as in an on-premises environment.
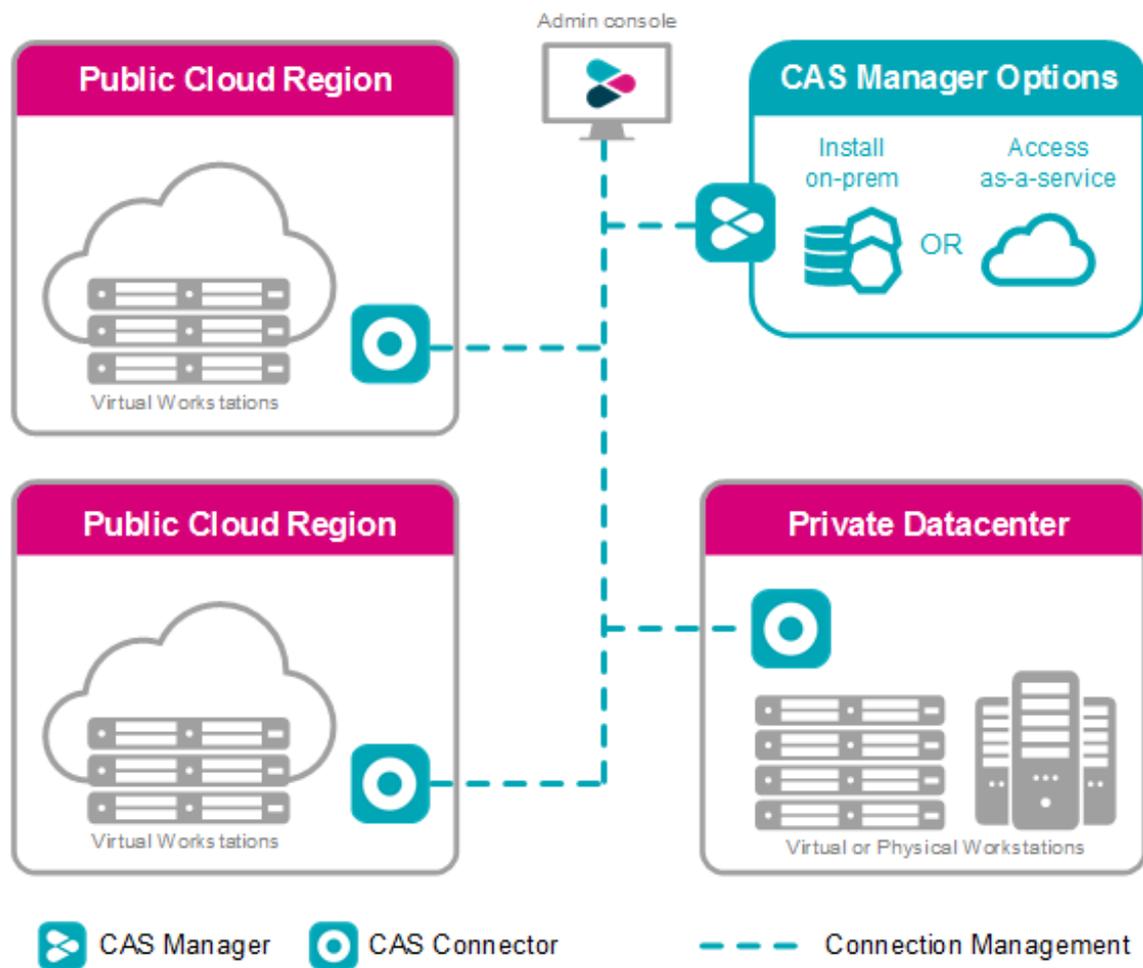
In addition to managing cloud compute costs, CAS Manager handles user entitlement, authentication (including RADIUS-compatible multifactor authentication (MFA)) and brokering of connections during PCoIP session establishment. The CAS Connector enables external users to access their remote desktops without the complexity of endpoint VPN´s.

2

Managed Connections for On-site LAN Users

LAN Users establish a PCoIP connection with a remote workstation by first connecting to an internally published IP address of the CAS Connector.
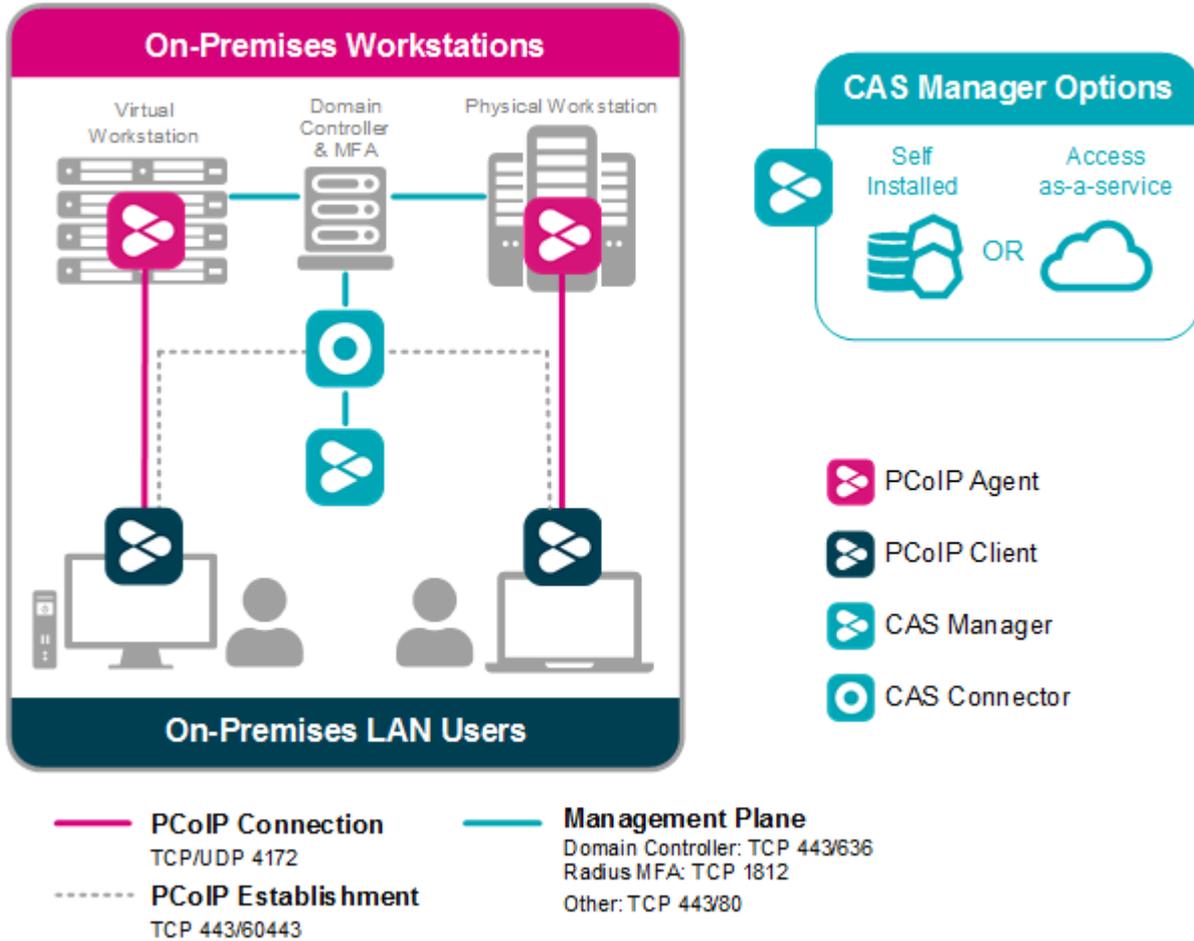

CAS Connector configuration details are described in the CAS Manager Administrators guide.

Managed Connections for WAN Users Connecting On-Premises

Off-site WAN users wishing to connect to on-premises remote workstations connect to an externally published IP address of the CAS Connector.

CAS Connector DMZ Deployment

The CAS Connector is conventionally deployed in a DMZ or semi-trusted zone (not shown in the diagram) and may be coupled with a reverse proxy to facilitate load balancing.
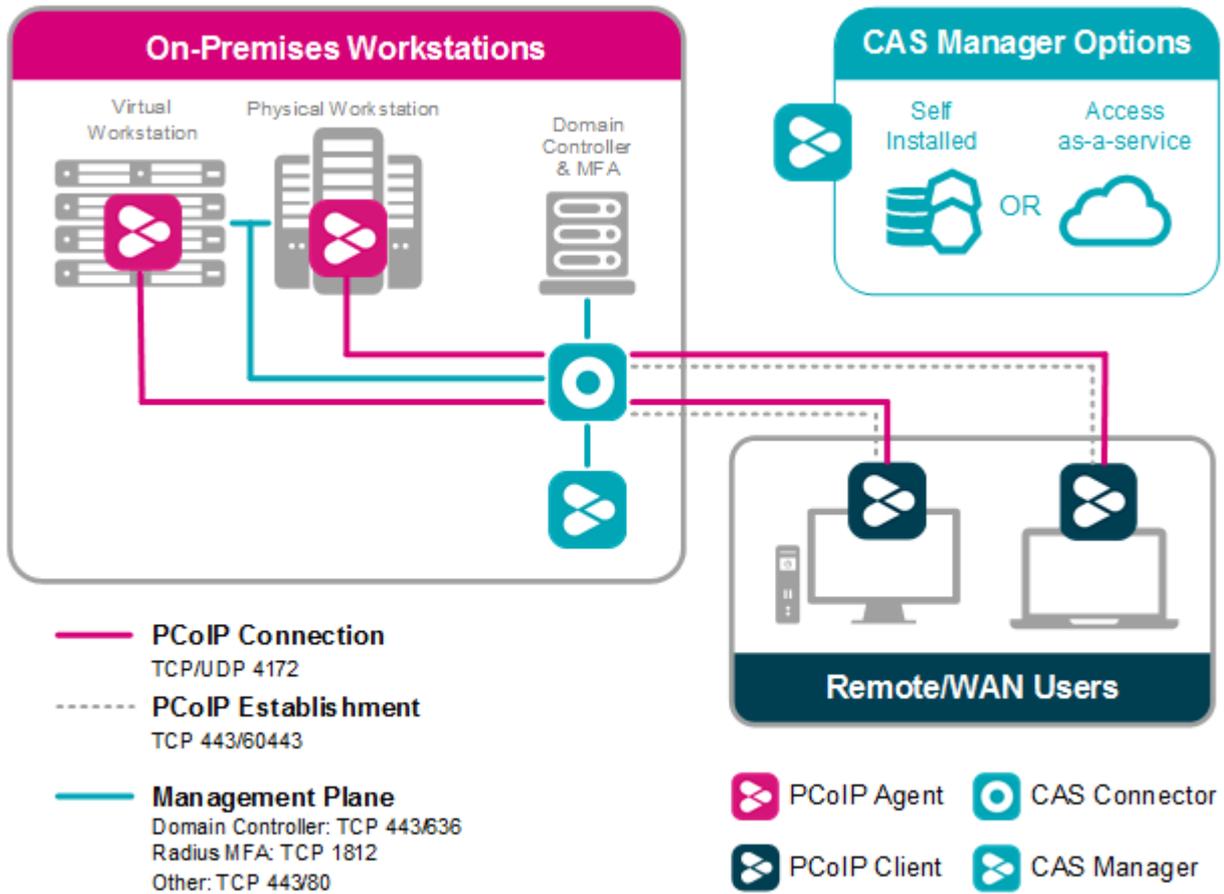
Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

**Managed Connections for Public Cloud Workstations**

CAS Manager supports connections to public cloud workstations. By deploying the CAS Connector in your preferred public cloud (in one or more regions and/or multiple public clouds), you can provide your on-site users with public cloud workstations or support users across different geographic regions with the nearest public cloud workstations. By choosing public cloud workstations situated geographically close to your remote users, the user experience is optimized.
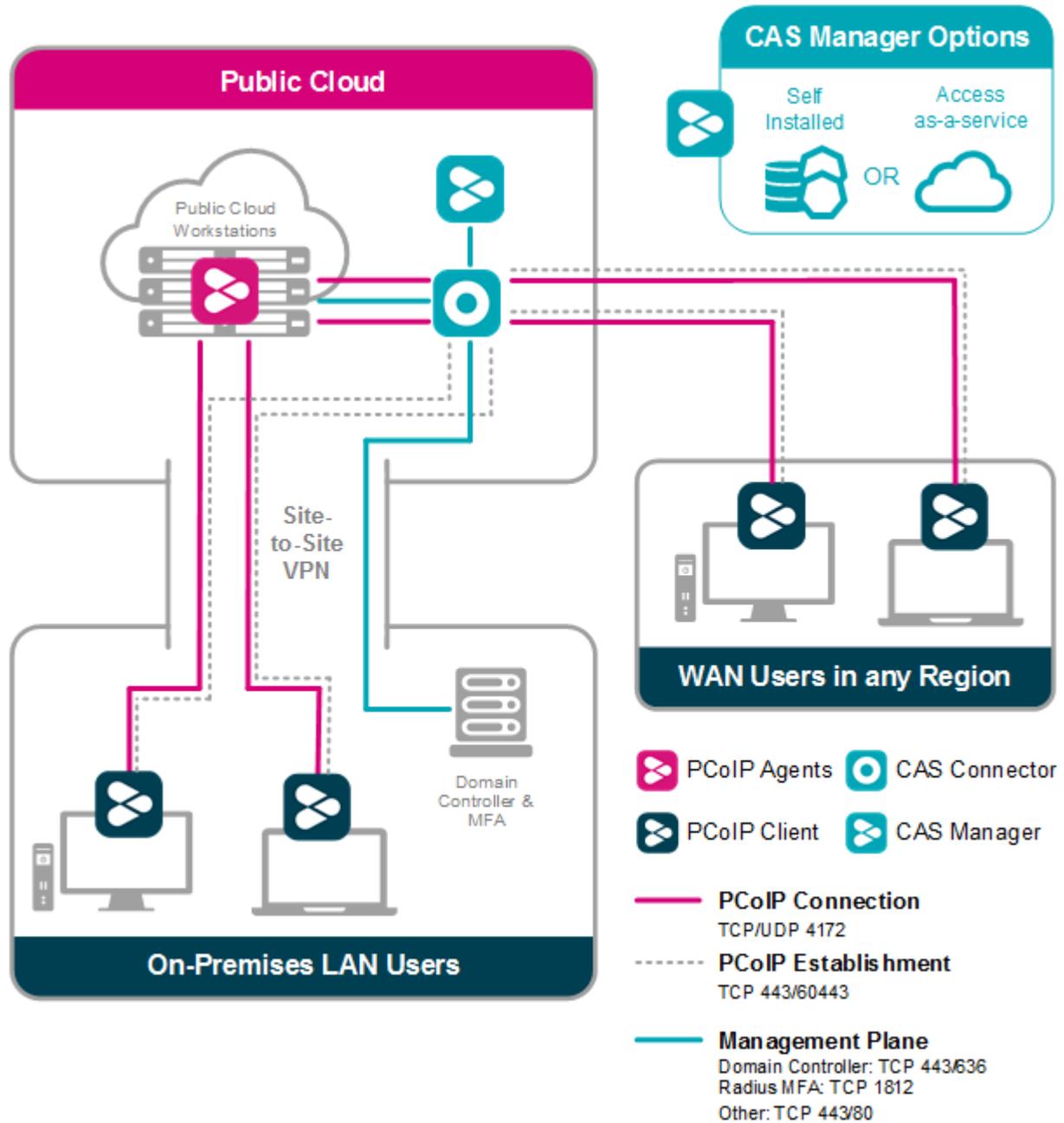
Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

**Managed Connections for Multicloud Workstations**

CAS Manager supports hybrid multicloud deployments comprising a combination of on-premises remote workstations (e.g. on VMware ESXi or KVM) and public cloud workstations in your preferred public cloud (in one or more regions and/or multiple public clouds). This is achieved by deploying the CAS Connector both on-premises and in one or more public clouds. By choosing public cloud workstations situated geographically close to your remote users, the user experience is optimized.
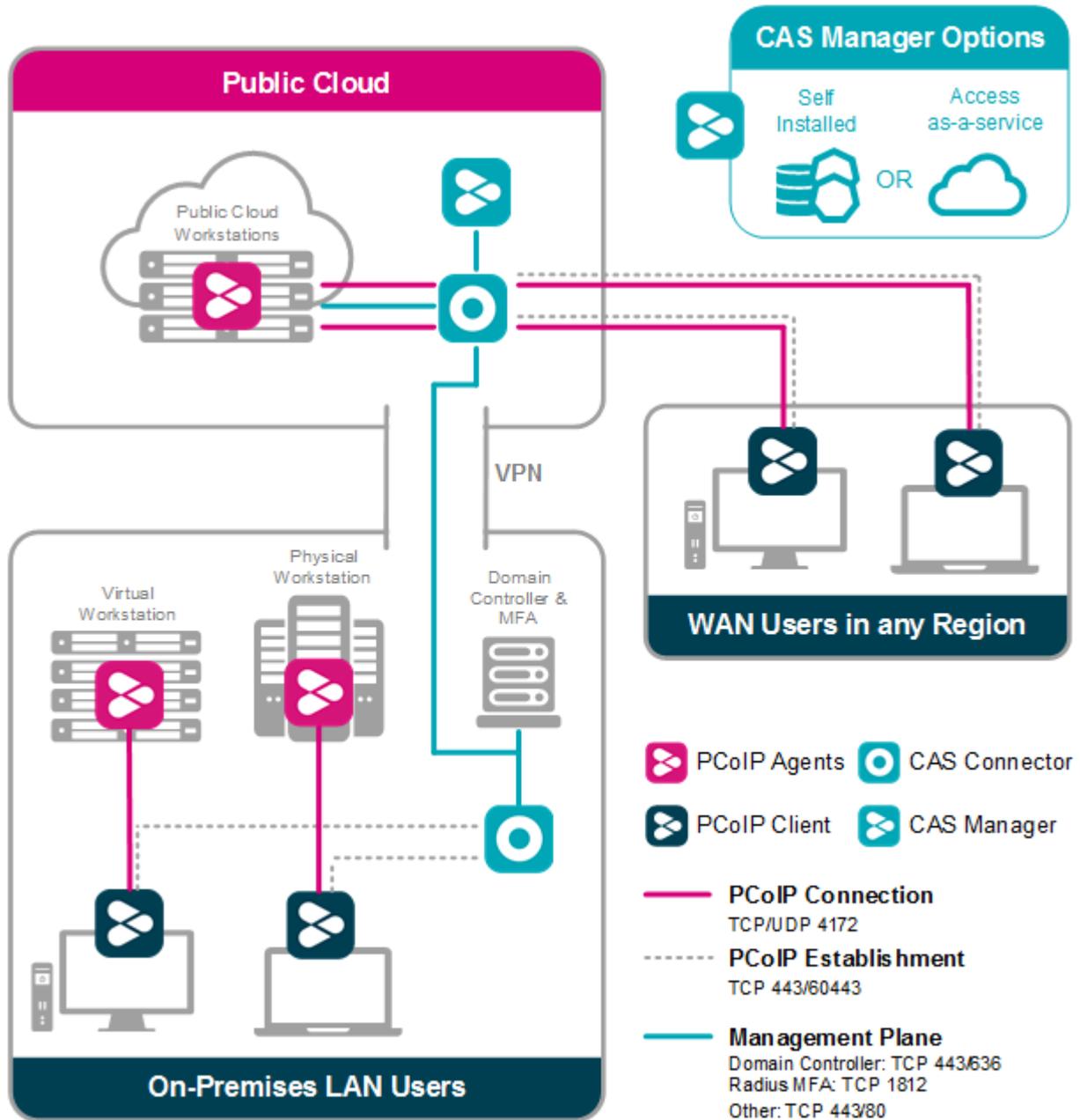
Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

Work-from-Home Options with Cloud Access Software

Teradici Cloud Access Software can offer a number of different solutions to your corporate work-from-home demands. The following image outlines a top-level architecture of the Work-from-Home scenario with Cloud Access Software:
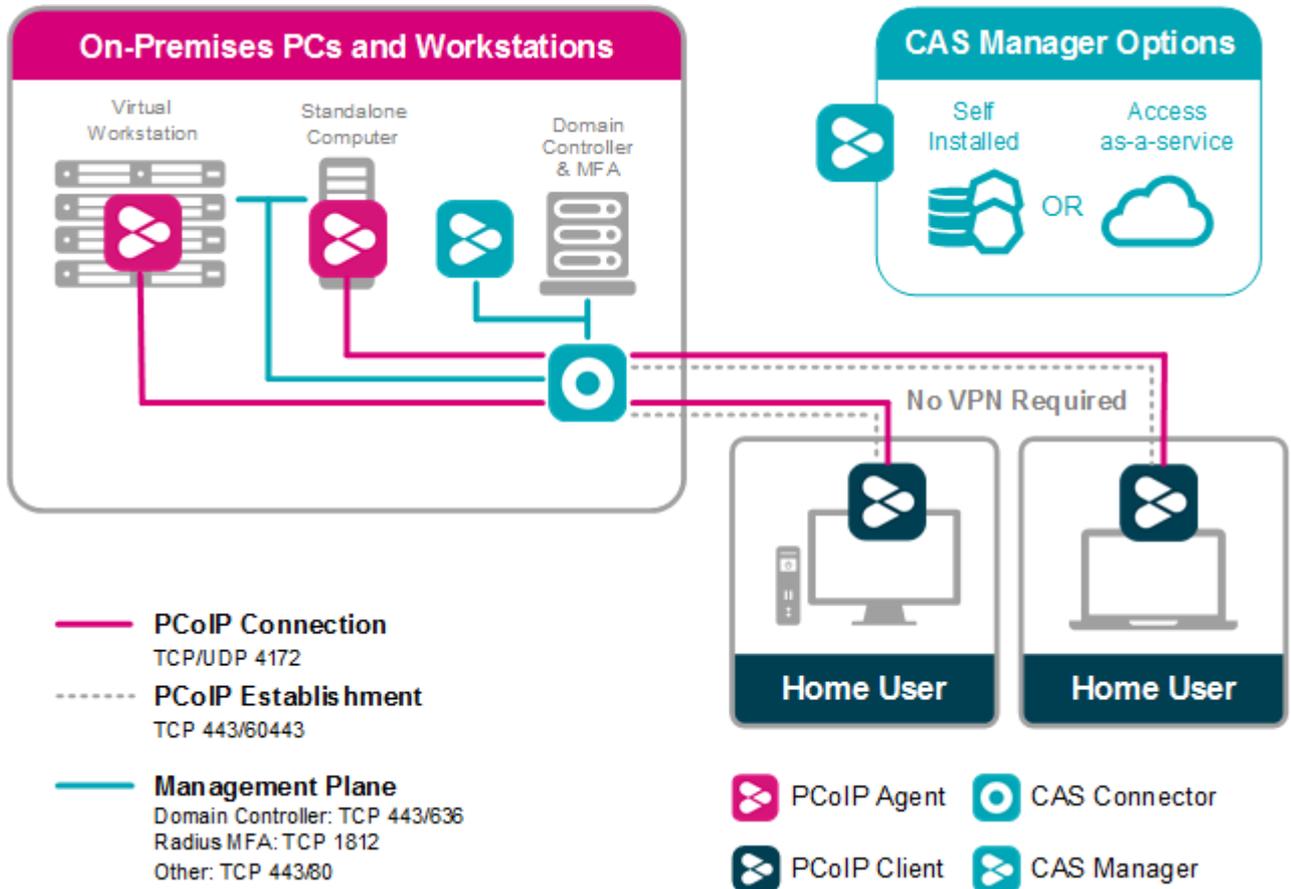
Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

For an in-depth view of our work-from-home offerings, please see our Work-from-Home Rapid Response Guide.

This guide outlines:

- Work-from-Home options for Standalone Computers.

- Work-from-Home options with Remote Workstation Cards.

- Work-from-Home options with Cloud Access Software.

- Work-from-Home options for VMware Horizon.

- Performance Tips for Work-from-Home Use Cases.