CLAROTY 安全远程访问 (SRA)

适用于工业网络可靠且融合的高度安全远程访问

工业网络远程访问的挑战

我们创建了 Claroty SRA 来解决 OT 远程访问的挑战。更具体地说，虽然 OT 远程访问是工业企业的关键必需品，但长期以来，由于三个重要原因，它一直存在风险和困难：

最终用户的复杂性：提高平均无故障时间

由于大多数传统的远程访问工具都是为 IT 网络设计的，因此它们通常具有繁琐的访问机制和接口，不适合 OT 需求。

在使用这些工具之前，最终用户不仅需要长时间的入职和培训，而且工具的复杂性和低效率意味着无论用户接受多少培训，他们可能仍然难以根据需求尽快修复工业资产。

这些条件增加了用户的平均无故障时间（MTTR），在必须立即进行紧急维修以避免或减少停机时间或其他严重后果的情况下，这可能会有问题。

管理员的复杂性：增加总体拥有成本

内部和第三方用户必须在需要远程访问工业资产时以进行维护或其他目的。

但是，管理此访问权限需要管理员维护成本高昂的复杂基础架构，同时满足用户的载入和故障排除需求。

第三方用户可能特别难以支持，因为他们通常无法与其他供应商的用户共享跳转服务器或其他基础架构，从而使管理员的工作进一步复杂化。

此过程即昂贵又耗时，对于 OT 环境而言，传统远程访问工具的总拥有成本（TCO）很高。

可视化和安全控制较差：增加风险敞口

OT 远程用户可能会进行未经授权的更改，从而给操作带来风险。使用传统的远程访问工具使网络安全人员无法了解用户的活动，并且无法使这些人员为用户实施基于角色和策略的访问控制，从而使这些风险变得更加复杂。

另一个问题，这些工具本质上是不安全的，因为它们往往使用易受攻击的 RDP 协议，并通过打破 Purdue Model 来违反工业网络安全，这是最佳做法。

因此，网络安全人员无法识别或控制谁从何处、何时或为什么登录。他们也无法识别或响应与这些用户活动相关的事件，所有这些都使 OT 环境面临更大的风险。

关于Claroty SRA

Claroty SRA 通过为内部和第三方用户提供对 OT 环境可靠且融合的高度安全远程访问，解决了 OT 远程访问的挑战。与传统的远程访问解决方案（其中大部分专为 IT 网络设计）不同，Claroty SRA 专为满足工业网络的特定操作、管理和安全需求而构建。

结果是一个独特的解决方案，可以减少平均修复时间（MTTR），最大限度地降低配置和管理 OT 远程用户访问的成本和复杂性，并减少 OT 环境因未托管、不受控制和不安全的访问而带来的风险。

主要优点

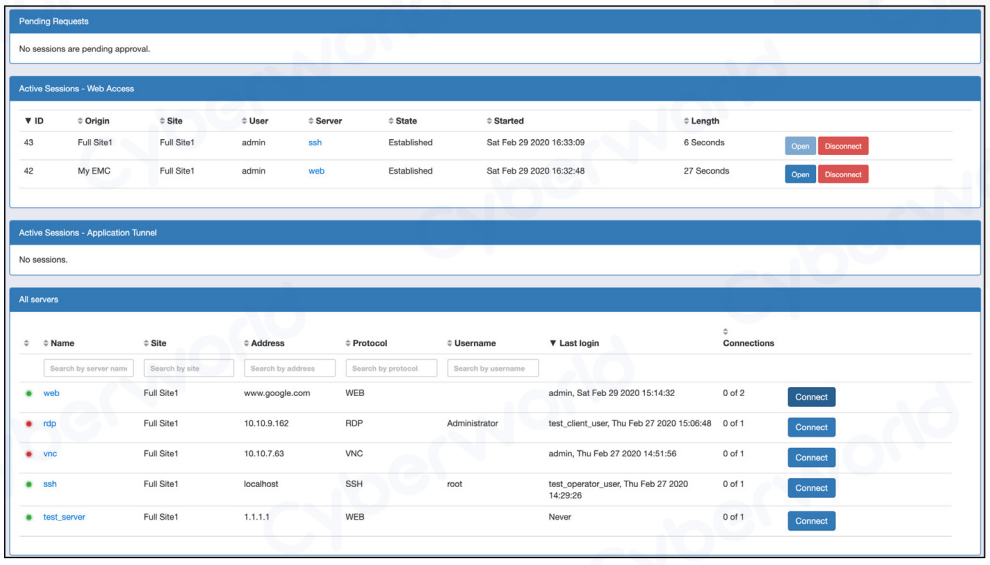
- SRA 通过随时随地更快、更轻松地连接和修复 OT、IoT 和 IIoT 资产来减少 MTTR 并延长正常运行时间。
- SRA 通过提供灵活的配置选项、集中式管理以及内部和第三方用户所需的一切，降低了安全、可靠、值得信赖的 OT 远程访问的复杂性和成本。
- SRA 使您能够控制、保护和了解网络中的所有远程连接和活动，从而最大限度地降低 OT 远程访问的风险。

SRA 特性和功能

降低平均无故障时间（MTTR）的用户体验

通过降低 OT 远程访问的最终用户复杂性，SRA 使用户能够在必要时更快更轻松地访问、排除故障和修复工业资产。
亮点包括：

- **准时制 （JIT） 用户配置：**SRA 通过 SAML 和 OpenID Connect （OIDC） 与各种身份供应商 （IdP） 集成，使管理员能够自动执行和简化 SRA 用户帐户的创建，作为单点登录过程的一部分。这意味着新用户可以自动添加到 SRA 并立即开始使用 SRA ， 所有这些都不需要管理员执行任何其他步骤。
- **高效的身份验证和访问：**SRA 还提供本机多因素身份验证，并且不使用跳转服务器。因此，授权的 SRA 用户可以在最需要的时候快速安全地进行身份验证和访问。
- **直观的界面：**SRA 界面反映了每个用户的本地技术体验，提供无与伦比的可用性，无学习障碍，也无需大量培训。
- **高可用性：**SRA 包括高可用性机制，确保用户无论在何种情况下都能保持访问权限。



具有活动远程连接的 SRA 主页视图

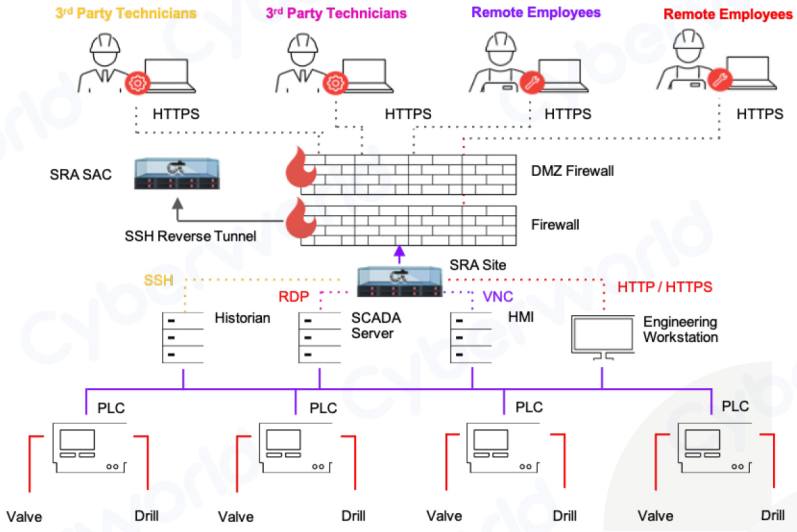
降低管理 OT 远程访问总体拥有成本的管理功能

SRA 通过提供灵活的配置选项、集中式管理以及内部和第三方用户支持其 OT 远程访问项目所需的一切，降低了管理员较高的 OT 远程访问总拥有成本（TCO）。亮点包括：

- **JIT 用户预配：**除了使 SRA 用户受益之外，JIT 用户预配还使 SRA 管理员能够通过自动执行为新 SRA 用户预配和保护访问以及载入的手动且耗时的过程来节省大量时间和资源。

- **灵活的部署和配置选项：**部署和配置 SRA 都不需要使用跳转服务器、复杂的防火墙规则或传统远程访问解决方案常见的昂贵且复杂的架构组件。因此，SRA 管理员可以花费更少的时间和金钱来部署和管理用户的远程访问基础架构，从而降低其总体拥有成本。

- **全面支持所有 OT 远程访问项目：**SRA 是真正的 OT 远程访问一站式解决方案，因为它包括支持所有 OT 远程访问项目所需的全部特性和功能。其中包括 OT 专用用户界面，用于多因素身份验证，密码保险存储，安全文件管理，高可用性，肩并肩监控等的多个选项。这意味着您可以满足内部和第三方用户的 OT 远程访问需求，而无需采购、部署和维护多个解决方案。



SRA 的部署体系结构示例，显示了对多种类型的远程用户的简单配置

访问和身份验证控制，将远程用户带来的风险降至最低

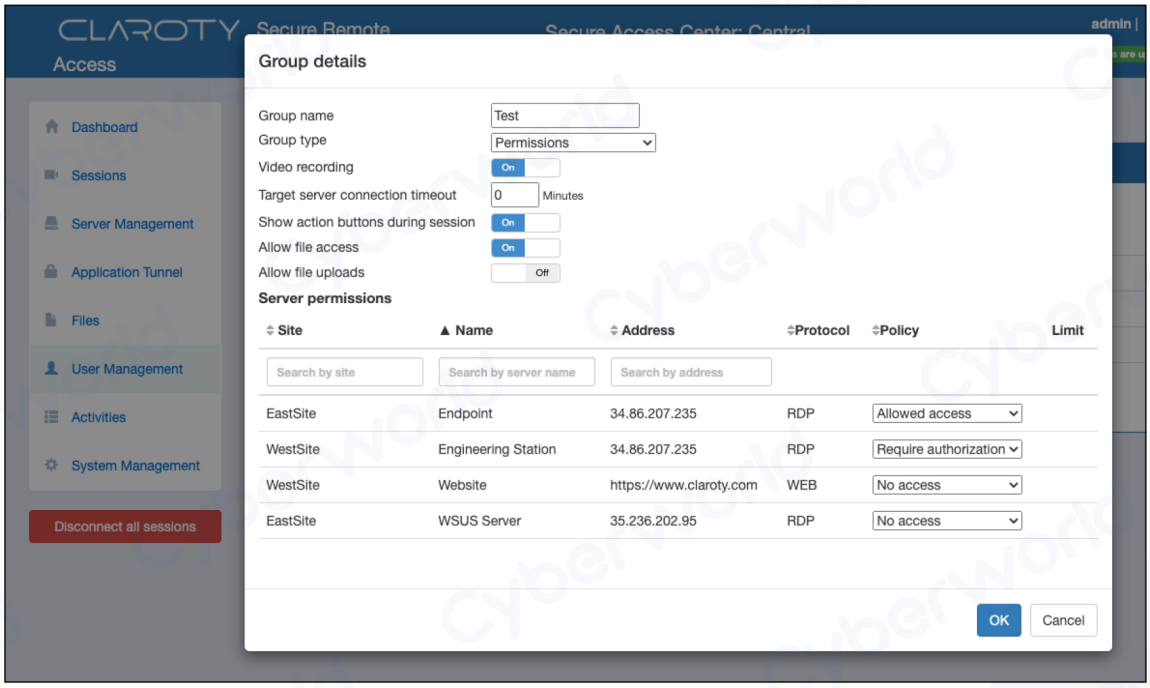
SRA 管理员可以跨多层控制访问工业网络，并具有特定性，以确定谁可以访问哪些资产、如何、何时、出于什么目的以及使用哪些协议。亮点包括：

- **安全身份验证：**SRA 包括本机多因素身份验证和凭据管理选项，支持实施密码的良性要求，并提供与基于 SAML 和 OIDC 的身份供应商集成的能力。

- **与身份供应商集成：**选择将系统与其现有身份供应商集成的 SRA 管理员可以自动将组织中已有的基于 SAML 或 OIDC 的身份验证策略和密码要求的实施扩展到其 SRA 用户帐户，从而确保 OT 员工和第三方的强用户身份验证。此功能还使前员工的 SRA 凭据自动失效，从而消除了特权提升和密码重用攻击中常用的高风险攻击媒介。

- **基于角色和策略的访问：**SRA 管理员可以在多个级别和地理位置为工业资产定义和实施极其精细的访问控制，最终简化用户工作流程，同时保护关键功能免受不必要的访问。此类控件支持零信任和最小特权安全原则。

- **安全批准和紧急访问：**对于远程访问时构成安全风险的资产，可以创建其他策略以确保每个资产环境的良好和可操作性。



SRA 显示的组织详情页面

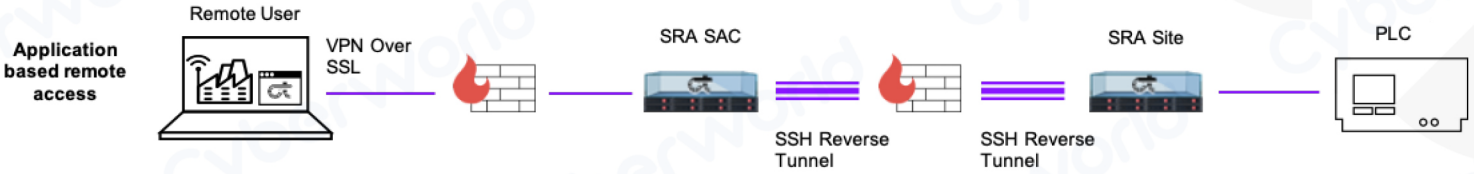
以固有的安全架构和功能来减少攻击面

将工业网络中的关键资产与外部连接隔离并主动防范恶意软件对于减少攻击面以及远程用户带来的风险至关重要。
SRA 通过以下方式提供这些功能：

- **对传输中的数据使用加密隧道：**SRA 将传输中的数据拆分到两个加密隧道之中，以减少连接到网络的设备数量、防火墙中开放端口的数量，从而减少攻击面。

- **保留 Purdue Model：**所有 SRA 部署选项都遵循保留 Purdue Model 的工业网络安全最佳做法，有助于确保一个连接点不提供广泛的网络访问。

- **杀毒解决方案集成：**SRA 与所有基于 ICAP 的杀毒解决方案集成。此功能通过提高对工业资产执行远程维护和相关任务所需的上传文件的安全性，帮助保护您的工业网络免受恶意软件的侵害。如果此类文件是恶意的，SRA 用户将立即收到通知，并阻止他们将其上传到相应的资产。



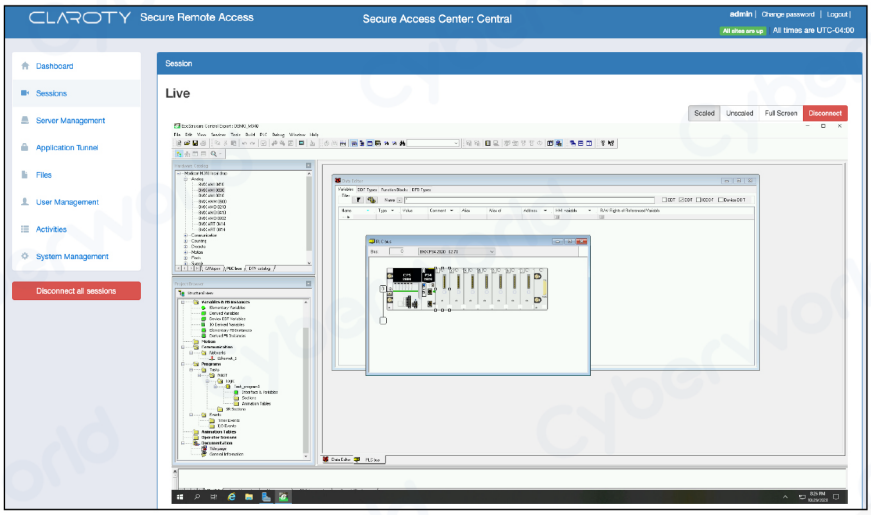
SRA 的加密隧道示意图

简化审计和优化调查的监控功能

通过提供远远超过大多数传统远程访问技术提供的基本日志记录功能和有限的审计跟踪的全面监视功能，SRA 让您能够全面地、实时地了解 SRA 用户的活动，简化审计并优化事件调查。亮点包括：

- **实时、肩并肩监控：**SRA管理员可以选择实时监控活动SRA会话，以便在必要时轻松排除故障、进行用户监控和紧急终止有风险的会话。

- **完整长度的视频记录：**除了保存所有远程会话的详细日志外，SRA还自动记录每个会话的完整长度的视频，以支持响应行动、调查和审计。



SRA 管理员对用户的 SRA 远程连接的实时、肩并肩监控视图

远程事件管理的广泛支持

SRA 与 Claroty 持续威胁检测(CTD)无缝集成，使 Claroty 平台成为业界第一个提供全面集成远程事件管理能力的工业网络安全解决方案。

这些功能跨越整个事件生命周期，使您能够从任何位置检测、调查和响应最广泛的可能的攻击面工业网络安全事件。因此，您可以针对远程、分布式和/或高度可变的工作环境，轻松地发展和调整组织的整体安全状况和工作流。亮点包括：

- **接收与 OT 远程用户活动相关的警报：**当用户通过 SRA 连接到工业网络时，当用户参与未经授权的或异常的活动时，如配置下载或在预定维护窗口之外服务资产，CTD 触发警报。这些警报包括 SRA 用户、会话意图、相关指标、涉及的资产、并进行根本原因分析，以支持优先排序和分类工作。

- **调查 OT 远程用户活动：**所有与 OT 远程用户活动相关的 CTD 警报都包括到相关 SRA 会话的直接链接，以及实时监控该会话的能力。如果会话不再活跃，警报将直接链接到一个完整长度的视频记录，可以查看调查目的。

- **回应 OT 远程用户活动：**与 OT 远程用户活动相关的所有 CTD 警报还使管理员能够在认为有必要作为响应操作时立即断开关联的 SRA 会话，以防止、遏制或补救因未经授权的更改或 OT 远程用户进行的其他活动而造成的任何损害。

所有由 SRA 用户活动触发的 CTD 警报都链接到相应的 SRA 会话，并使管理员能够查看，如果认为有必要，可以直接从 CTD 的警报视图页面断开会话

CLAROTY

Cyberworld
广州科明大同科技有限公司
中国区总代理

官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

关于Claroty

Claroty 是一家工业网络安全公司。Claroty 深受全球性大型企业的信赖，可帮助客户揭示、保护和管理其 OT、IoT 和 IIoT 资产。它的综合平台与客户现有的基础设施和计划无缝连接，同时提供全方位的工业网络安全控制，以实现可视化、威胁检测、风险和漏洞管理以及安全远程访问， 所有这些都大大降低了总拥有成本。Claroty 得到了领先的工业自动化供应商的支持和采用，拥有广泛的合作伙伴生态系统和屡获殊荣的研究团队。

了解更多，请访问 www.claroty.com