



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。

它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、更轻松连接和修复OT、IoT、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

通过降低最终用户OT远程访问的复杂性，SRA使用户能够在必要时更快、更轻松访问、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，并立即使用SRA，这些都不需要管理员执行其他步骤。
- 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操作体验，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。

The screenshot displays the SRA dashboard interface. It is divided into several sections:

- Pending Requests:** A section at the top indicating that no sessions are pending approval.
- Active Sessions - Web Access:** A table listing active web access sessions. It includes columns for ID, Origin, Site, User, Server, State, Started, Length, and buttons for Open and Disconnect.
- Active Sessions - Application Tunnel:** A section indicating that there are no active application tunnel sessions.
- All servers:** A table listing all servers with columns for Name, Site, Address, Protocol, Username, Last login, and Connections. It includes search filters for server name, site, address, protocol, and username.

ID	Origin	Site	User	Server	State	Started	Length	Open	Disconnect
43	Full Site1	Full Site1	admin	ssh	Established	Sat Feb 29 2020 16:33:09	6 Seconds	Open	Disconnect
42	My EMC	Full Site1	admin	web	Established	Sat Feb 29 2020 16:32:48	27 Seconds	Open	Disconnect

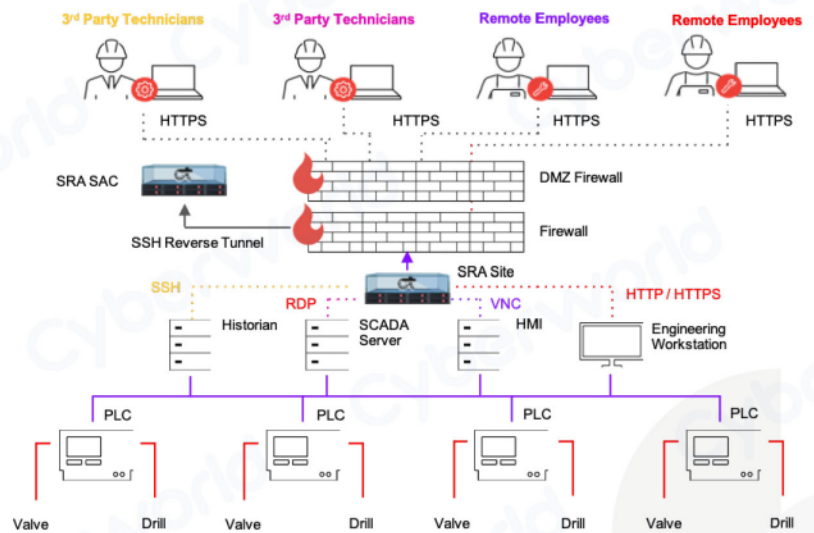
Name	Site	Address	Protocol	Username	Last login	Connections
web	Full Site1	www.google.com	WEB	admin	Sat Feb 29 2020 15:14:32	0 of 2
rdp	Full Site1	10.10.9.162	RDP	Administrator	test_client_user, Thu Feb 27 2020 15:06:48	0 of 1
vnc	Full Site1	10.10.7.63	VNC	admin	admin, Thu Feb 27 2020 14:51:56	0 of 1
ssh	Full Site1	localhost	SSH	root	test_operator_user, Thu Feb 27 2020 14:29:26	0 of 1
test_server	Full Site1	1.1.1.1	WEB		Never	0 of 1

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远程访问总体拥有成本(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，减少了手动且耗时的 workflows，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、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专用的用户界面、多因素身份验证、密码保险存储、安全文件管理、高可用性、实时监控等的多个选项。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。



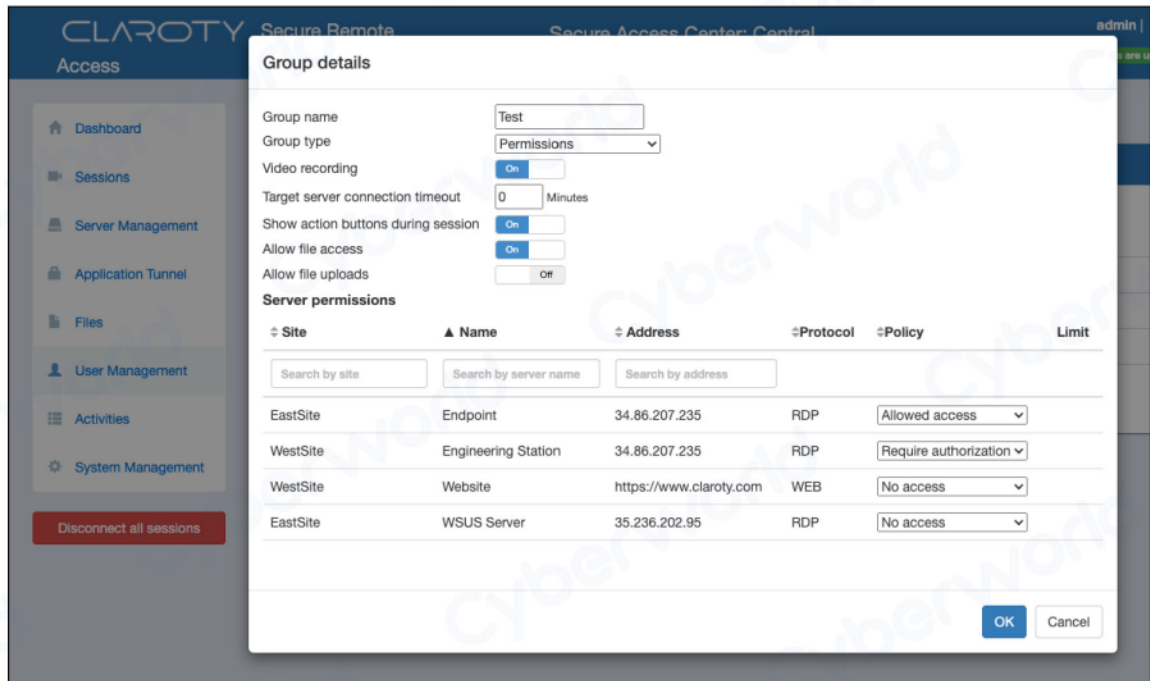
SRA 的部署体系结构示例，显示了对多种类型的远程用户的简单配置

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，支持实施密码管控要求，并提供与基于SAML和OIDC的身份供应商集成的功能。
- **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，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，消除了特权提升和密码重用等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，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

将工业网络中关键资产与外部连接隔离，主动防范恶意软件。这对于减少攻击面和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。
- **保持使用普渡模型：**所有SRA部署选项都遵循使用普渡模型，这是工业网络安全的最佳实践，可确保是一个连接点，而不是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。此功能可以提高对工业资产执行远程维护、相关任务所需上传文件的安全性，保护您的工业网络免受恶意软件侵害。如果发现恶意文件，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。

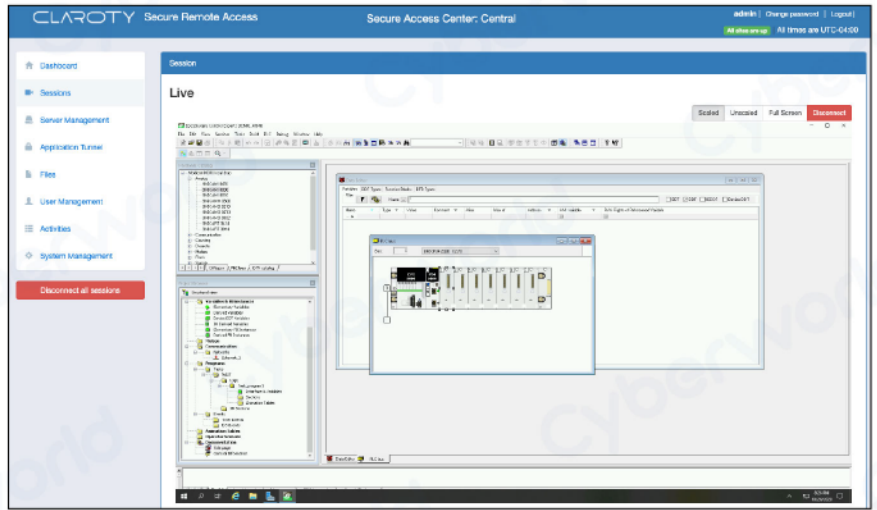


SRA 的加密隧道示意图

简化审计和优化调查

Claroty SRA远远超过大多数传统远程访问的技术，它能提供基本的日志记录功能和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：

- **实时监控：**SRA管理员可以选择实时监控会话，以便在必要时轻松排除故障。在紧急情况下，可及时终止有风险的会话。
- **完整的视频记录：**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视频，以支持响应行动、调查和审计。



SRA 管理员对用户的远程连接的实时监控页面

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平台成为业界首个提供全面集成远程事件管理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、调查和响应最广泛攻击面的工业网络安全事件。因此，您可以针对远程、分布式和可变的工作环境，轻松地发展和调整组织的整体安全状况和 workflows。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，参与未经授权或异常活动（例如配置下载或在预定维护时段之外维修资产），CTD会触发警报。这些警报包括以下详细信息：SRA用户、会话意图、相关指标、涉及的资产以及支持优先级和分类工作的根本原因分析。
- **调查 OT 远程用户活动：**与OT远程用户活动相关的所有CTD警报，都包含指向关联SRA会话的直接链接以及实时监控该会话的功能。如果会话不再处于活动状态，警报将直接链接到完整的视频记录，可以出于调查目的进行查看。
- **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，可以使管理员能够在认为必要时立即断开关联的SRA会话，作为响应操作，以防止、遏制和补救未经授权的更改造成的任何损害，或OT远程用户进行的其他活动。



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。如果管理员认为有必要处理，可以直接从CTD的警报页面断开会话。

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使工业、医疗保健、商业机构、大型企业和公建部门能够保护其环境中的所有网络化物理系统——扩展物联网 (XIoT)。Claroty平台可以与客户现有的基础设施集成，提供可视化、漏洞和风险管理、威胁检测、安全远程访问的全方位控制。Claroty得到了全球领先的工业自动化供应商的支持和采用，拥有广泛的合作生态系统以及屡获殊荣的Team82研究团队。