KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert
July 30, 2021

PortSys Total Access Control

Zero Trust Architecture requires proper authentication and authorization for each access request in the digital domain. Access management tools must serve ever more complex environments ranging from contemporary cloud hosted applications as well as legacy on-premises applications that do not conform to current access control standards in order to meet strategic Zero Trust initiatives. PortSys Total Access Control is an access management solution that can help customers improve their authentication, authorization, and Single Sign-On capabilities and integrate with existing identity repositories.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Businesses, government agencies, and non-profit organizations of all sizes have increasingly complex requirements for managing access to their digital resources. With cybercrime and fraud growing in volume and sophistication, access management has become a front-and-center issue for executives, managers, and users alike.

Access management solutions generally contain a core set of functions including authentication, authorization, identity federation, and Single Sign-On (SSO). Access management is a large subset of Identity and Access Management (IAM), which encompasses identity proofing, provisioning, credential issuance, identity repositories, lifecycle management, governance, entitlements management, access reconciliation, deprovisioning, and audit.

Client-server access management was well established by the turn of the millennium and relied upon the fairly static generation and maintenance of users, groups, and roles. Entitlements were coarse-grained permissions contained in Access Control Lists (ACLs). Web access management evolved to meet the different technical requirements of that environment, which largely utilized browser cookies, HTTP headers, and encoded URLs as workarounds for the lack of notions of statefulness and user identity in the online world. Identity federation arrived in the early 2000s to enable SSO between web domains. Authorization and entitlement management have been extended to allow more fine-grained, attribute and policy-based access controls.

Many legacy applications still need to be supported and need to cooperate with enterprise access management systems. For legacy apps that do not work with IAM solutions, a common alternative is to place the application infrastructure behind reverse proxy server(s). In this scenario, the application servers and databases are generally located on isolated VLANs, with a reverse proxy mediating access to the legacy application. The reverse proxies are configured to intercept user requests, interact with authentication and authorization services, and allow or deny access in accordance with enterprise policies.

Each of the areas within broader IAM and access management specifically have been componentized and offered "as-a-Service" by vendors. Adherence to pertinent IAM standards allows interoperability between products and service providers. Some products and services offer discrete functions such as authentication; others serve as Identity Providers (IdP)s, addressing the functions of identity verification, credential issuance and maintenance, governance and lifecycle, etc.; and yet others offer the full stack of IAM capabilities. Some vendors in the IAM space were early to not only support cloud-based applications, but also to create cloud-native identity services, often called Identity-as-a-Service (IDaaS). While current IAM products and IDaaS solutions cover a large percentage of use cases, many organizations still struggle to integrate modern IAM systems with non-standard client-server (legacy) applications.

Besides having a wide range of possible applications, data types, and user identity repositories, managing access is further complicated by the fact that organizations need to allow users outside their home organizations "in" to their resources, which may be in their data centers or in various cloud locations. Depending on the use cases, employees, contractors, B2B customers, and consumers may need to be managed. Moreover, these additional users access resources from disparate types of devices, many of which are not under the control of the target enterprise. Device identity, reputation, and health can and should be considered as attributes in access control decisions.

Authentication has been one of the areas within access management that has experienced the most technical advancement. Researchers and vendors have sought to address the inherent weaknesses of password-based authentication and have thus developed many different kinds of authenticators and protocols to increase assurance levels. Biometrics on mobile devices, out-of-band applications, mobile push notifications, and a variety of hardware tokens are noteworthy examples.

Authentication and authorization services, as two key ingredients in access management solutions, are important threads in Identity Fabrics, which are gaining traction in industry today. An Identity Fabric is an architecture that can be composed of disparate data sources and capabilities delivered as discrete services. Identity Fabrics permit organizations to add and upgrade segments of their infrastructure or contract with service providers to meet business objectives in a more agile manner. Given the widespread availability and adoption of cloud-hosted services running the gamut from IaaS to PaaS to SaaS, more vendors are packaging their solutions in containers such that they can provide the same types of functions regardless of deployment models. This means that on-premises software ships as images or virtual instances that can be deployed on most of the common operating systems or IaaS/PaaS platforms or made available as micro-services via the vendor or MSPs.

Zero Trust Architecture (ZTA) has arisen over the past decade and has become a primary means of addressing access control use cases. ZTA, usually shortened to "Never trust, always verify", is an embodiment of the principle of least privilege, and at its core mandates that every access request be properly authenticated and authorized. Thus, access management is a foundational element for ZTA. Proper access management in service of ZTA means taking into account the requesting user's attributes, authentication context, environmental context, permissions and roles, source device information, and the requested resource attributes. Zero Trust Architecture implies a concept where clients can access services from everywhere, not relying only on internal network security mechanisms and IAM. In fact, ZTA has become the strategic IT security paradigm for many services and products.

The key requirements most organizations look for in ZTA-enabling access management solutions are:

- Support for multiple authenticator types, such as:
    - Smart Cards, USB tokens, and older form factor hardware tokens
    - Mobile apps and push notifications
    - x.509 certificates
    - Biometrics, especially mobile biometrics leveraging native OS capabilities

    - OTP: HOTP/TOTP over phone, email, and SMS

- Availability of a mobile SDK for customers to write their own secure apps
- Adherence to policy-based access control model so that IT departments and Line of Business application owners can define risk-appropriate access control rules
- Enforcement of configurable actions including permit, step-up authentication, deny, lock account/device, etc.
- Integration with legacy applications using proprietary means and other IAM systems to allow SSO, usually via cookie support
- Support for identity federation via OAuth2, OIDC, JWT, and SAML
- Integration with SIEM, SOAR, UBA, and other security systems
- Provide administrators with management dashboards and configurable reporting
- Allow for delegated and role-based administration within the solution

2 Product Description

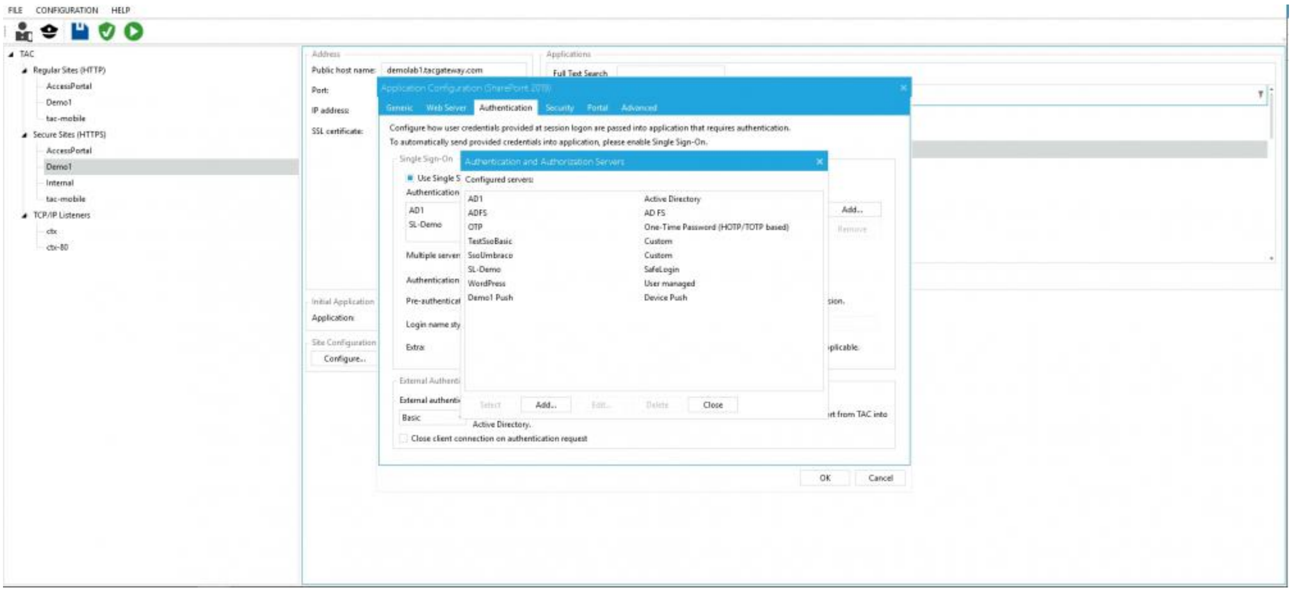
PortSys is a privately funded company that was founded in 2008 and based in Marlborough, Massachusetts. PortSys started out building security appliances with Microsoft and HP and has evolved to provide Zero Trust Access Controls to a variety of commercial organizations and government agencies in North America and the EMEA regions. PortSys' solution utilizes reverse proxy-based access controls that can be deployed on-premises, in the cloud, or in hybrid environments. Unlike pure IDaaS and CASB solutions, they provide solutions for client-server and legacy apps.

PortSys Total Access Control (TAC) is delivered in the form of hardened, Windows-based virtual appliances that can be installed on-premises, in the cloud, or across hybrid environments: on customer hardware, in AWS or Microsoft Azure, or on VMware or Hyper-V. For scalability, up to 64 virtual appliance nodes can be configured as a single array. Moreover, multiple arrays can be deployed in a load-balanced, high availability (HA) cluster, in either active/active or active/passive modes. Licensing for the product is based on numbers of annual user subscription blocks, instead of being based on numbers of deployed virtual appliances, logins, or utilization, as is common for authentication services. PortSys does not charge extra for HA configurations.

TAC is not an IdP, rather it acts as access management gateway that can rely upon traditional IAM and IDaaS solutions. TAC supports the primary identity and federation standards and protocols: LDAP, SAML, OAuth, and OIDC. These allow interoperability with Microsoft Active Directory (AD), Microsoft Active Directory Federation Server (ADFS), Microsoft AD Azure, Okta, Ping Identity, and One Login services. TAC provides SSO capabilities for IaaS instances and popular SaaS apps, such as Microsoft O365, Google GSuite, Box, Dropbox, Salesforce, etc.

TAC can be an authentication gateway for proxied applications; in this case, TAC handles authentication and users get the appropriate level of access directly after the authentication event. TAC instances can also serve as portals for various user groups, depending on the individual customer's needs. The look and feel of the portal is configurable. TAC ships with 17 themes which can be white labeled for consistent branding and further customized with CSS. TAC supports all major browsers. TAC has a built-in self-service password reset utility. Each user can personalize their portals with saved searches and favorites. After authentication, portals load with a tailored view of the applications, file shares, and other resources to which each user has been granted access. TAC's portal approach makes it easy and more efficient to find the specific applications, tools, or other resources they need to work with regularly.

In all cases, TAC appliances serve as an authentication portal. PortSys offers its own SafeLogin strong authenticator, a picture-recognition based method that obviates the need for passwords. Other MFA options available in TAC include SMS OTP, mobile push notifications, Swivel Secure, RSA SecurID, Thales SafeNet, OneSpan Digipass, Cisco Duo Security, PinSafe, Smart Cards, and x.509 certificates. FIDO 2 and universal server support is planned for TAC in September 2021. Authentication policies can be defined to require different mechanisms based on resource sensitivity. The policy authoring interface features drop down list selection for mapping groups, roles, and authenticator types. Customers construct policies to evaluate user, requesting device, target resource, and environmental attributes using Boolean logic.



Public host name: demolab1.tacgateway.com

Configure how user credentials provided at session logon are passed into application that requires authentication.
To automatically send provided credentials into application, please enable Single Sign-On.

Authentication: AD1, SL-Demo

Configured servers:

AD1	Active Directory
ADFS	AD FS
OTP	One-Time Password (HOTP/TOTP based)
TestSsoBasic	Custom
SsoUmbraco	Custom
SL-Demo	SafeLogin
WordPress	User managed
Demo1 Push	Device Push

Active Directory.

□ Close client connection on authentication request

Figure 1: PortSys TAC management interface for application configuration (courtesy of PortSys)

VPN utilization had been growing for years, but with the rapid shift to Work From Home (WFH) as a result of the pandemic, VPNs have become the principal means by which many employees and contractors do their jobs. Many if not most SMBs and enterprises were unprepared for the massive increase in VPN utilization and the security issues it generated. Organizations with username/password only VPN authentication found themselves at high risk for Account Takeover (ATO) attacks and subsequent loss of intellectual property from data exfiltration. TAC supports RADIUS authentication, which has historically been the standard protocol for network layer access. The solution is often deployed in customers' perimeters. Employees and contractors navigate to the customer portal, authenticate in accordance with administrator defined policies, and can be granted access to resources. TAC brokers authentication with internal IAM servers or IDaaS providers.

Moreover, TAC can take the place of VPN solutions. As a reverse proxy, a TAC deployment can allow granular access to enterprise resources after appropriate authentication and authorization. Thus, TAC can allow customers to reduce or eliminate VPN connectivity. VPNs without proper network segmentation and/or without tight integration with existing IAM infrastructure can expose organizations to increased risk of compromises and data breaches. The PortSys approach of offering a reverse proxy with integrated authentication and authorization may help some customers move away from less secure VPN installations and move toward Zero Trust Architecture.

In addition to augmenting or replacing VPNs for remote access, TAC can function as an access hub for SSH jump boxes, Microsoft RDP services, and Citrix XenApp and Xen Desktop. TAC supports clientless HTML5 based RDP as well.

Managed Security Service Providers (MSSPs) have successfully deployed TAC as a means to control access to their customers' resources. MSSPs are by definition security conscious and must strictly limit where their employees can go and what they can do within their customers' domains, so as not to become an attack vector themselves. MSSPs can set up TAC portals to present their analysts with links to the administrative utilities, including command-line tools over SSH, in customer environments for which they are authorized. Moreover, different authentication policies can be constructed per customer to comply with individual requirements.

PortSys' TAC uses a reverse-proxy architecture, where the TAC virtual appliances are inserted into customer networks logically in front of the resources to be protected. The reverse-proxy model allows TAC to protect legacy applications and data stores that do not work well with modern IAM infrastructures. Many organizations run older applications which do not receive timely or regular support. Others have key line of business applications that are heavily customized COTS products with complex dependencies on homegrown code and databases. Examples of such legacy apps can include inventory management, manufacturing controls, power generation, and financial application. Legacy applications present more security risks than merely the lack of interoperability with contemporary IAM systems. Legacy apps sometimes run on older operating systems and may therefore have many more exploitable vulnerabilities. Adherence to Zero Trust means separating these resources into more easily defensible locations and enforcing strong authentication and access control. TAC helps clients achieve ZTA in legacy environments by serving as the identity aware gatekeeper.

TAC can proxy any HTTP/HTTPS traffic, and supports TLS 1.2, 1.1, 1.0, and SSL 3.0. TAC can inspect and modify incoming HTTP/HTTPS requests and filter out misconfigured headers and prevent certain common kinds of web application attacks such as Cross Site-Scripting (XSS). TAC uses FIPS 140-2 certified crypto components. Each virtual appliance contains an integrated firewall. TAC can perform a number of important risk analyses for each incoming request:

- Operating system patch level
- Check for presence of endpoint protection clients and signature levels
- Check for presence of Unified Endpoint Management (UEM) and Mobile Device Management (MDM) clients and installed device certificates
- Perform geo-fencing based on client IP address

For management, PortSys provides a single dashboard for statistics and a base set of common reports. Applications can be published to distinct user communities by means of a publishing wizard. PortSys provides tools to migrate customers to their solution from other application gateway products. The admin interface supports export and import of policies in a proprietary format to speed bringing new TAC instances online.

PortSys interoperates with Security Incident and Event Management (SIEM) solutions by passing log information via syslog. Customers can choose to protect the TAC admin interface with the same MFA options that are available for ordinary users. Various admin roles can be created permitting controlled access to different resources.

3 Strengths and Challenges

The need for strong MFA options continues to grow in response to Account Takeover attacks, data breaches, ransomware, and other cyber threats. Tighter access controls can help reduce the risk of the loss of intellectual property.

PortSys focuses on delivering highly integrated authentication and authorization solutions that interoperate with the major on-premises IAM systems and cloud-hosted IDaaS. TAC supports the right mix of identity standards and protocols to facilitate connections with not only leading IdPs, but also many SaaS apps. The reverse-proxy deployment model enables TAC to serve as a secure gateway front-ending legacy applications that do not interoperate with contemporary security and identity tools. TAC can be a component in a Zero Trust Architecture. The virtual appliance form factor makes it easy for customers to deploy and manage. The ability to deploy up to 64 TAC appliances in clustered and load-balanced arrays allows for excellent scalability. PortSys offers migration utilities to help move customers onto their solution.

TAC would benefit by exposing the authentication service via APIs and offering a mobile SDK for customer app development. TLS 1.2 and prior are supported, and TLS 1.3 support is in the testing stage. Demand for TLS 1.3 will likely increase. MSSP customers would benefit by having connectors available from TAC to the leading SOAR solutions.

Small-to-medium sized businesses as well as enterprises and government agencies with limited IT support and organizations with the need to expand remote access for employees and contractors may find PortSys TAC to be a compelling access management product.

PORTSYS®
Zero Trust Access
for the Modern Enterprise

Strengths

- Hardened virtual appliance with built-in firewall facilitates scalability and high availability
- Integrated VPN access management enables customers to rapidly add strong authentication mechanisms for remote worker and contractor use cases
- Adherence to Zero Trust Architecture design principles
- Customizable portals allow for brand consistent appearance
- Once authenticated, each user’s authorized apps and resources display in the portal
- Good selection of MFA types to meet varying levels of authentication assurance
- SafeLogin’s picture recognition authentication method helps move customers away from insecure passwords
- Migration tools aid implementation

Challenges

- No authentication service API or mobile SDK
- TLS 1.3 support planned for late 2021
- Linux-based OSes for the virtual appliance may be appealing to some customers
- No connectors for SOAR solutions

4 Related Research

Leadership Compass Enterprise Authentication

Leadership Compass Access Management

Buyer's Compass Access Management

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.