Accops Hysecure - Datasheet

Introduction

HySecure Gateway is a platform-agnostic, comprehensive remote access and security gateway solution designed to provide secure, flexible, and scalable access to corporate resources for on-premises, remote workers and distributed teams.

With a focus on advanced security features, ease of management, and support for various deployment scenarios, HySecure enables organizations to adapt to the evolving needs of a modern workforce while maintaining robust protection against cyber threats.

Product Overview

HySecure offers a unified platform for secure remote access, combining robust security measures with user-friendly management tools. Key components include:

- **Zero Trust Access Control**: Implements a zero-trust security model with continuous verification and least privilege access principles.
- **Application Support**: Compatibility with a wide range of applications and protocols, including SaaS applications.
- **Access Security**: Advanced Encryption, Authentication, Web Application Protection, Tamper Proofing, Advanced Bot Management and Access Control Mechanisms.
- **Management**: An intuitive web-based management console featuring graphical reporting and automated alerts.
- **Authentication**: Multi-factor authentication with support for various methods, including biometrics and push notifications.
- **Auditing**: Comprehensive logging and reporting for compliance and security monitoring.
- **Authorization**: Granular access control based on user roles, device profiles, location, network etc.
- **Endpoint Control**: Real-time device status checks and compliance enforcement.
- **Access Modes**: Multiple access modes cater to diverse user needs and device types.
- **Deployment**: Flexible deployment options include on-premises, virtualized, and cloud-based environments

Features and Benefits

Application Support

- All Web-based, TCP, and UDP-based client-server applications
- Windows file shares and drive mapping
- Dynamic port-based applications
- Publish the Subnet or IP Range for network access
- Special support for RDP virtual channels
- Application server load balancing
- Session caching for load-balanced applications
- Per application-based compression switch
- MyDesktop for direct personal desktop access
- Terminal server application & VDI publishing via RDP & VNC, HyWorks
- HyWorks VDI & Hosted Application
- SAAS based Application support, including Microsoft 365, Google Workspace, and Salesforce
- VoIP (voice over IP) Application
- Fileshare
- SSO (SAML Support)
- Office 365, GSuite, Salesforce (MFA is supported)
- Contextual Access to Applications based on user, device, location, and time

Access Security

- Support for TLS 1.3
- Encryption:
    - Strongest available: DES, 3DES, AES
    - State-of-the-art quantum-safe encryption algorithms
- Authentication: SHA-2, RSA 2048/4096
- 4096-bit RSA key CA certificate support
- Endpoint security trust level
- Internet network masking and IP address/hostname mangling
- Application-level Access
- Hardened gateway operating system
- Split & Full tunnel modes
- Secure sandbox computing
- DDOS Protection
- Device-based application access for Office 365, Salesforce & Outlook
- Continuous verification of user identity and device security posture
- Adaptive Risk-Based Access Policies: Dynamic authorization based on real-time risk assessment
- Web Application Protection (WAP): Comprehensive security approach designed to protect web applications and APIs from a wide range of cyber threats including:
    - OWASP Top 10 Web Application Security Risks, OWASP Top 20 Automated Threats and SANS 25 Software Errors.
    - Over 4000+ built-in signatures on various technologies, platforms and frameworks with pre-defined templates.
    - Certificate Revocation Lists (CRLs) verify whether a digital certificate has been revoked before its expiry by the issuing Certificate Authority (CA).
    - Automatic learning and profiling application structure. Threat scoring and baseline creation for AI driven zero-day attack protection.
    - Anti-bot protection with AI classification and scoring of bots based on advanced browser fingerprinting.

- Built-in AV scanner for malicious file upload. Support for ICAP integration for 3rd party scanners.
- Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, URL, country, etc.
- Built-in XML firewall, validation of XML / JSON / Ajax / SOAP / GraphQL /REST API requests and WebSocket requests.
- Tamper rules for URL / parameter tamper protection, website defacement, hidden form field protection, cookie signing and encryption, etc.
- Support for protection against buffer overflow attacks, man-in-the-middle attacks, blocking malware payload, SQL, SSI, LDAP injection, etc.
- Protection against invalid HTTP requests.
- Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts.

Management

- Self-signed certificate generation
- Certificate-based strong authentication for administrators
- Bandwidth usage
- Auto backup on E-mail/FTP
- Support for Notification based on user access, Account lockout support, Access control expiry
- Features like Client Auto-Upgrade, Broadcast Customized messages
- Application Heath and Resource Monitor and Alert
- Email Notifications for Device Approval Status
- REST API Support: Integration with third-party management and security tools
- Early Notification for Idle Timeout
- Features like smart reconnect, intelligent session timeouts, and secure desktop access with one-time URLs
- Web-based management console with a dashboard and graphical reporting
- Smart analytics dashboard to ensure session details, User identity, authentication, and MFA details, device posture, application availability through proactive health monitoring.

Authentication

- Authentication based on user identity, OU/group/realm
- Static passwords, OTP - dynamic passwords
- Certificates
- Strong device identification based on over 20 parameters, including HOSTNAME, VERSION OF AGENT, OWNER, CPUID, USERID, MBID, OS HDDID, MACID, IMEI Number, DEVICE ID, MODEL and STATE.
- User location, MAC ID, IP Address
- ADFS Support
- SAML Integration
- Two-factor authentication:
  - Certificates, Device Signatures
  - One Time Passwords (OTP): SMS/Email/Hardware/Biometric/Software Token
  - Local database with full customization per user, password policies & reset support
  - RSA Secure ID or any 3rd party OTP server
  - Fully integrated client-certificate-based two-factor authentication server with automatic CA and certificate provisioning
  - Email-based user provisioning
  - Support for multiple authentication servers with cascading mode
  - Realm-based multi-organization support
  - SAML-based SSO

    - Biometric authentication
    - Consent (Push Notification)
    - Consent with additional tokens (Push Notification)
    - SSO NPLM-based apps
- Google Secure LDAP Service Integration: Authentication without Active Directory dependency
- SSH Password Management: Options to set and reset SSH passwords
- OAuth/OpenID Connect Support: Integration with modern identity providers
- Passwordless Authentication: Support for FIDO2/WebAuthn standards

Auditing

- Detailed logging of time of access, username, domain, MAC Address of endpoint, IP address of endpoint, application accessed, device profile, and productivity logs
- User location monitoring (Accops Reporting Server - ARS)
- Monitor users for log monitoring
- Complete reporting of user logons and activity
- Detailed logging of endpoint security scan results
- Extract logs in CSV format for third-party report generation
- Search logs
- Auto-archiving of logs
- Monitor and disconnect live users
- Alerts on new device registrations, user account lockouts
- Reporting on domain-wise access, applications accessed, failed login attempts, and concurrence graph
- Alert on Resource Utilization
- Syslog support
- Advanced Analytics Dashboard: Visualization of access patterns and security events
- Compliance Reporting: Pre-built reports for regulatory compliance requirements

Authorization

- Access control based on device identity and profile, endpoint security trust level, user authentication method, user role, user's organization, user's location
- ACL (Access Control List) expires automatically
- Application-based access control
- Dynamic policy evaluation based on runtime information about device, authentication methods, and user roles
- Display of allowed applications and availability of the application server to users
- Time-based restriction policies
- Scheduled account expiry
- Block specific groups
- Multiple VPN domain-based control
- Control the User's Internet access
- Support for external authorization servers
- Automatic fetching of group information from AD/LDAP
- Attribute-Based Access Control (ABAC): Dynamic policies based on user and device attributes
- Just-In-Time Access Provisioning: Temporary access rights for specific tasks

Endpoint Control

- Real-time status check for last update time, real-time protection check, process check
- Detect managed and unmanaged devices
- Login control from managed and unmanaged devices

- Support of login through MDM-managed devices (VMware and other MDM solutions)
- Support for checking OS Version, antivirus, firewall, and antispyware products
- Geo-fencing, Domain Joined
- IP Address-based access control
- Windows update-based access control
- Registry key, client certificate base posture check.
- Application control based on device profile
- Mandatory profile for non-avoidable policy checks on all endpoints
- Quarantine profile for devices that fail other profiles
- Secure endpoints from attacks over the Internet
- Agent with Built-in Tamper Protection like stop agent services, modify configuration file, password on installation and uninstallation, running as a service.
- Restricted Internet access of users based on policy
- Restrict data leakage using the clipboard, printing, and USB devices
- Geo-location-based restriction
- Windows update-based restriction
- Profile-based security policy
- **Enhanced Device Compliance Checks**: Comprehensive Compliance Verification
- **Browser Security Extensions**: Additional security for web-based access
- **Device Posture Assessment**: Continuous monitoring of endpoint security status

Access Modes

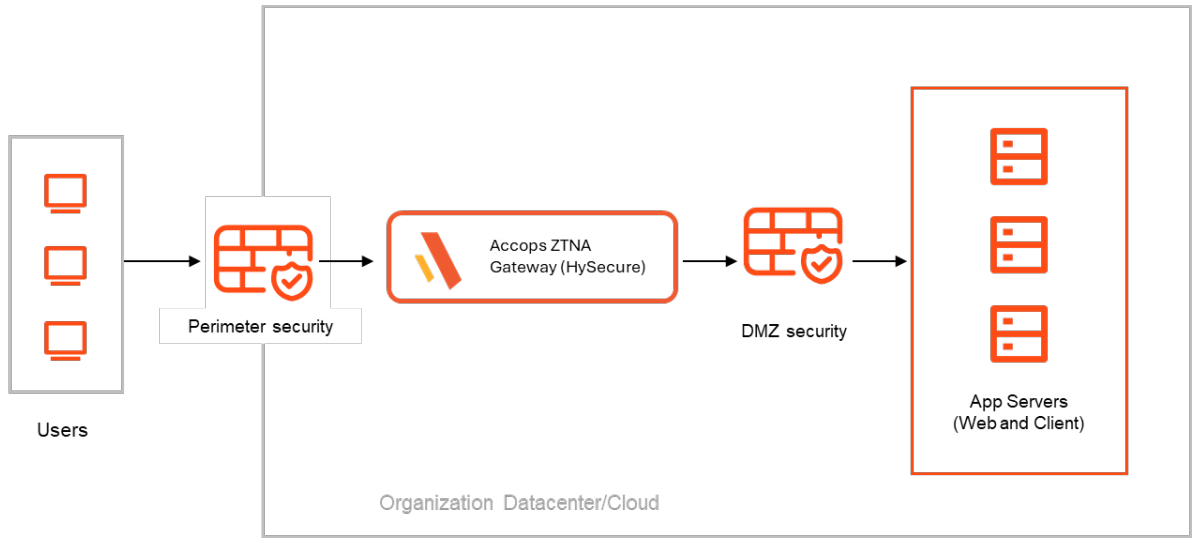
- HyLite HTML5 portal for clientless access
- Agent-based access from any browser
- Full access client for desktops
- iOS & Android mobile apps
- Hybrid Portal Mode
- L3 VPN Mode
- Reverse proxy Clientless VPN for web applications
- Client platforms supported: Windows 7/8/10/11, Windows Server 2012R2/2016/2019/2022, Linux OS, macOS, iOS/iPadOS, Android
- No configuration required on end user machines
- Site to site access
- Hostname-based Reverse Proxy App Support
- New Turbo Tunnel for L3 VPN
- Seamless SSO for Web Applications
- Built-in Remote Desktop Gateway

Platform Support

- Runs on hardened Linux based platform
- Supported on any standard or custom hardware. Also, support to run on Purpose Build Appliance (directly onto bare metal)
- Supported to run on virtualized platforms from VMware ESXi, XenServer, Hyper-V, Nutanix AHV, Proxmox, Red hat OpenShift. Also, various cloud platforms like AWS, Azure, Oracle Cloud, Google Cloud,
- Kubernetes-based deployment for cloud-native environments
- Multi-Zone/Region Deployment

Deployment type

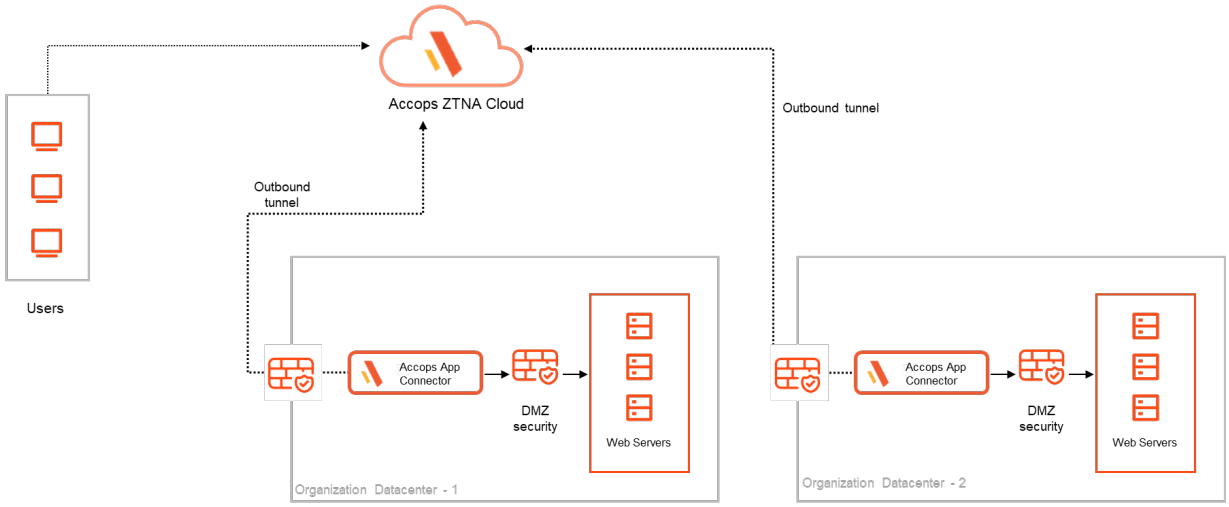
Inbound ZTNA Deployment:



The On-Premises Inbound Deployment Model enables secure remote access to internal applications through a single, controlled entry point within the organization's datacenter. External users connect to a designated public IP that terminates at a secure gateway deployed behind the perimeter firewall. The gateway authenticates users, enforces role-based access policies, and securely proxies traffic to internal applications, ensuring that backend servers are never directly exposed to the internet.

By centralizing access through the on-prem secure gateway, organizations significantly reduce their attack surface while maintaining full control over infrastructure, data residency, and compliance requirements. The architecture simplifies firewall configurations, provides complete visibility into user activity (who accessed what and when), and aligns with Zero Trust principles by enforcing identity-based access rather than traditional network-level trust.

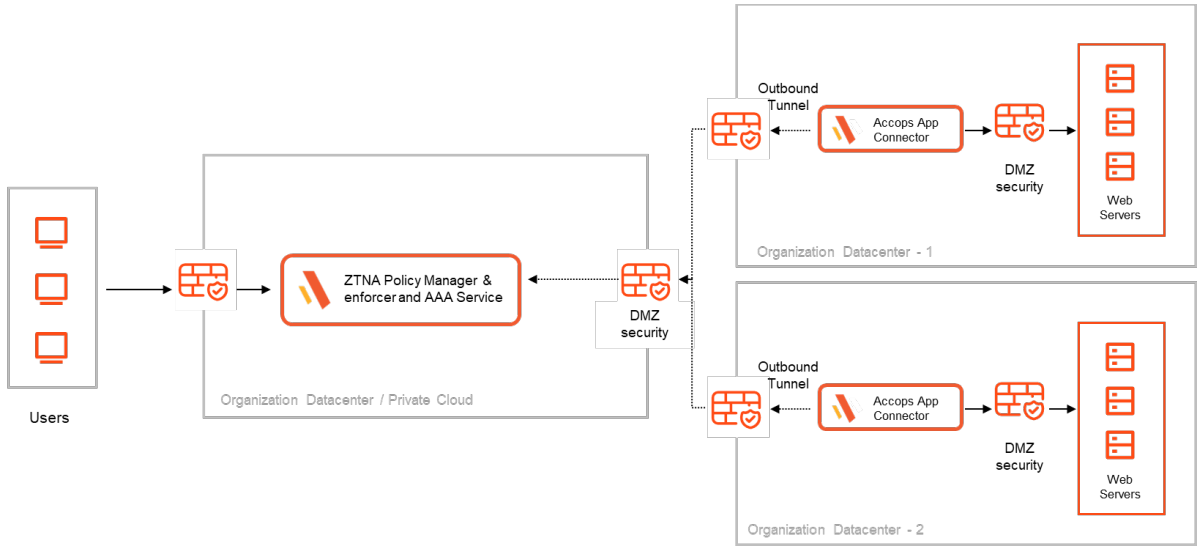
Reverse Connect - Outbound ZTNA Deployment (Cloud or As-a-Service):



This Deployment Architecture provides secure, identity-driven access to applications hosted across one, two or multiple datacenters without directly exposing backend servers to the network. All user and inter-service requests are routed through a single whitelisted public IP that terminates on a secure gateway (Accops ZTNA Cloud Plane). The gateway performs authentication (SSO/AD/IdP integration), enforces role-based access policies, and inspects traffic before securely forwarding it to the appropriate internal application. Backend server IPs remain completely hidden, and direct connectivity to application servers is never permitted.

Policy orchestration, centralized visibility, and access governance are managed through the Accops ZTNA Cloud Plane, which acts as the centralized control plane across all datacenters. This ensures uniform policy enforcement, consolidated audit logs (who accessed what and when), and simplified administration regardless of location. The architecture reduces firewall rule complexity, minimizes the attack surface, and aligns with a Zero Trust model by enforcing identity validation, device awareness (if enabled), policy-based routing, and optional controls such as DLP, download restriction, and session monitoring.

Reverse Connect - Outbound ZTNA Deployment (100% On-Premises or Organization Private Cloud):



Following the same principles as cloud deployments based on a Reverse Connect Topology, the entire solution is architected to be deployed 100% on-premises within the organization's datacenter environment. In this model, application connectors initiate outbound secure connections to the gateway/control plane, eliminating the need for inbound firewall openings while maintaining full control within the enterprise network.

This design ensures that organizations can achieve the same Zero Trust security posture, centralized policy management, and secure application access capabilities as cloud deployments—while retaining complete ownership of infrastructure, data residency, and compliance requirements within their on-premises datacenters.

Conclusion

- **Enhanced Security**: Robust security features including multi-factor authentication, advanced encryption, and real-time threat detection.
- **Zero Trust Architecture**: Verify-first approach to security with continuous validation of every access request.
- **Flexible Deployment**: Support for on-premises, virtualized, and cloud-based deployments to meet diverse organizational needs.
- **Remote Workforce Support**: Secure access for remote workers across various devices and platforms.
- **Integration Capabilities**: Integration with leading identity and access management systems for a seamless user experience.
- **Certified and Compliant**: Compliance with industry security standards and certifications to ensure reliability and trust.
- **Simplified User Experience**: Intuitive access to resources without compromising security.
- **Reduced Cost of Ownership**: Consolidated solution for remote access needs with centralized management.

Accops enables secure and instant remote access to business applications from any device and network, ensuring compliant enterprise mobility for business users while keeping governance with the organization.

Want to learn how Accops can help you secure critical applications, business data, and ensure compliance?
Reach us at contact@accops.com