DATASHEET

Secure SD-WAN by Open Systems provides all the benefits of SD-WAN while reducing cyber risk, simplifying regulatory compliance, and eliminating the headaches associated with managing an «ecosystem».

Secure SD-WAN packages

	Business	Enterprise	Enterprise Plus
SD-WAN Base	X	X	X
Bandwidth Control	X[1]	X	X
Path Selection	X[1]	X	X
Application Acceleration		X	X
DNS Filter	X[2]	X	X
Firewall		X	X
Secure Web Gateway		X	X
Network Security Analytics		X	X
Network Security Monitoring			X
Unified Threat Protection	X	X	X[3]

SD-WAN Base

Integrated Service Management

Service Delivery Platform

- Industrial strength hardware
- Hardened operating system
- Multi-release boot configuration for fallback and recovery

Design and deployment

- Definition of technical configuration
- Definition of the administrative contacts and escalation procedures
- Creation of a site checklist
- Creation of the network topology diagram
- Preconfiguration, delivery and functional verification tests of the deployed services with all required hardware and software components

24x7 monitoring and operations

- 24x7 proactive monitoring, event notifications (by email or SMS), automatic log file analysis and reporting
- Prompt response to detected critical events
- Unlimited number of escalations, tickets, support calls
- Direct support by Open Systems Security Engineers

1 Limited scope

2 Standard policy

3 Advanced Threat Protection Feeds

Change management

- Enforced change management processes by comprehensive ticketing system and built-in sign-off procedures
- Review of change requests by Security Engineers, clarifications and feedback in case of hidden risks
- Strong user authentication with audit trail

Troubleshooting and maintenance

- Real-time auditability with integrated ticketing system
- Debugging of incidents within the periods defined in the SLA
- Replacement of defective or outdated hardware and restoring of functionality
- Analysis, testing and installation of software patches and upgrades
- Predefined disaster recovery processes

Reporting and logging

- Real-time executive overview with geographic distribution
- Real-time reporting of configuration settings and logs
- Real-time network utilization and system load statistics
- Compliance report: Service Organization Controls 1 Type 2 (SOC 1)

Coverage of technology risk

- Hardware and software are replaced free of charge if defective, outdated or if the quality or availability of the implemented systems are no longer guaranteed by the manufacturer

Open Systems Customer Portal

- Strong user authentication with audit trail
- Delegated administration
- Ticketing
- Real-time monitoring and reporting
- Strong user authentication with audit trail
- Full audit log
- Backup to customer storage backend
- Real-time view of operational key figures and statistics
- View of relevant configurations
- Self-service and debugging tools

WAN Encryption and Routing

- Secure site-to-site connections through the internet, MPLS, VSAT or other WAN transport layers
- Full and partial meshing
- Star and explicit topologies
- VPN tunnel monitoring with latency and packet loss statistics
- Static and dynamic routing
- Route propagation to LAN
- Graphical and statistical connection monitoring
- Service and ISP outage escalation
- High availability via automatic failover and real-time data synchronization

DHCP Server

- DHCP Server: standalone, local network configuration allocation
- DHCP Relay: centralized, local network configuration allocation
- High availability via automatic failover and real-time data synchronization

Application Visibility

- Overview of all applications on the network
- Bandwidth usage per application in local scope and company wide
- Drill-down of company-wide application overview to sites and specific applications

Bandwidth Control

- Globally defined profiles that are instantiated for every location
- Priority classes for each profile
- Up to 15 subclasses per profile
- Application assignment to subclasses
- Flexible queue allocation for optimal bandwidth usage at class and subclass level
- Guaranteed throughput per subclass
- Maximum bandwidth definition per subclass

Path Selection

- Dynamically manage the path of application data in the network and over multiple links
- Globally defined profiles that are instantiated for every location
- Priority classes for each profile
- Up to 15 subclasses per profile
- Application assignment to subclasses
- Individual routing policies per subclass
- Routing selection priorities over more than two ISP links

Application Optimization

- Combination of redundancy elimination and optimization techniques:
  - compression
  - deduplication
  - caching
  - network protocol optimization

DNS Filter

- Inspection of every DNS query
- Blocking of DNS queries resolving disallowed domain names
- Blocking policy based on domain name categories
- Configurable error page
- Blacklisting and whitelisting

Firewall

- Global firewall zoning concept
- Globally deployed firewall policy with capability for local exceptions
- Two separate policies included (e.g. WAN and DC)
- Dynamic IP groups
- Real-time view and history of the firewall configuration
- Advanced log viewer for real-time and historical data
- Global packet tracker utility
- IP and protocol-based filtering
- Domain-name-based filtering
- Application-based filtering

Secure Web Gateway

- HTTP proxy server
- FTP proxy server
- Proxy auto configuration (PAC)
- Group access policy enforcement
- Port access policy enforcement
- Configurable error pages
- Global internet access policy enforcement
- Advanced log viewer for real-time and historical data
- URL Tracker
- IPv6 compatible
- Up to 5 dedicated proxy policies

User Authentication

Kerberos

- Microsoft integrated authentication against Windows Active Directory server
- Kerberos v5 mechanism
- Assignment of Internet Policy membership via LDAP attributes

LDAP

- Client authentication against LDAP server using browser pop-up window
- LDAP bind to server
- Assignment of Internet Policy membership via LDAP attributes

Malware Protection

- Malware scanning
- HTTP/FTP protocol scanning
- Archive handling policies
- Media type filters

Advanced Malware Protection

- Detection of rapidly evolving malware with artificial intelligence
- Real-time classification of advanced threats in the cloud
- Inspection of executable files only

URL Filter

- Enforcement of corporate internet access policy
- Cloud-based URL filter
- Category-based filtering
- Blacklisting and whitelisting

SSL Scanning

- Policy enforcement for encrypted traffic
- Server certificate validation with customized action
- SSL certificate mimicking
- Client certificate tunneling

Web Traffic Tap

- Export of HTTP and decrypted HTTPS traffic for passive network security monitoring
- Simulated network traffic between proxy client and web server, observable on designated network interface
- Full visibility of request headers and full responses

Network Security Analytics

- Global event collection
- Threat score algorithm
- Notification of high threat score
- Global dashboard
- Local dashboard for delegated administration
- Drill down from global overview to event details
- Host view including context information
- Self-provisioned event categorization
- Self-provisioned whitelisting for events and hosts
- Combination of protocol, signature and anomaly-based inspection
- Multiple sources of threat intelligence signatures
- Customized detection patterns
- Packet capture utility
- Inspection of encrypted HTTPS traffic in combination with the Secure Web Gateway

Network Security Monitoring

This package includes Network Security Analytics as well as:

- Notification of high threat score to Open Systems Mission Control operations
- Process-based event validation and classification by Open Systems Mission Control operations
- Process-based escalation by Open Systems Mission Control operations

Unified Threat Protection

Unified Threat Protection consists of selections of threat intelligence feeds of different focus that are consumed by the subscribed Open Systems services:

- basic protection, which is included in Secure Email Gateway, and in Secure Web Gateway and DNS Filter packages of Secure SD-WAN
- advanced protection, which offers Additional Threat Protection Feeds, an add-on with a per-user fee

For more information, see the «Unified Threat Protection» datasheet.

SD-WAN deployment types and capacities

Type	Users per site	Service SLA
Class 1 site	> 800	99.95%
Class 2 site	200 – 800	99.95%
Class 3 site	20 – 199	99.95%
Class 4 site	20 – 199	99.4%
Class 5 site	< 20	99.4%
Cloud		99.95%

Open Systems services are ISO 27001 certified.