Acronis SCS

WHITEPAPER - SEPTEMBER 2019

Deploying Acronis SCS Backup Software in Networks with Firewall Segmentation

A Practical Guide for US Public Sector Organizations of All Sizes

For Sales & Technical Inquiries:
info@acronisscs.com
1-877-202-0240

OVERVIEW

Acronis SCS's backup software is often deployed in networks with strict firewall segmentation. The benefits of segmentation are well established; in fact, they are often considered a key step in an organization's adoption of a zero trust framework.

This whitepaper describes and illustrates four common network scenarios across a variety of environments – from small- and medium-sized organizations, state agencies, and municipalities to large enterprises and federal agencies.

It should serve as a resource for your network administrators and IT staff as you plan the layout of your computing environment, no matter your organization's size, including the deployment of your management server and agents within your segmented network.

Acronis SCS Backup 12.5 and our upcoming hardened backup product are designed to work within these varied environments. Our software requires minimal network firewall rule requirements and, in some cases, the port used to access your web management console can be changed to better support your environment's layout.

If you run a network with more complex network segmentation than is shown here, this guide should still be helpful for identifying which ports must be allowed and where. Simply combine the below layouts to match the specifics of your environment (see Appendix A for a complete network flow guide).

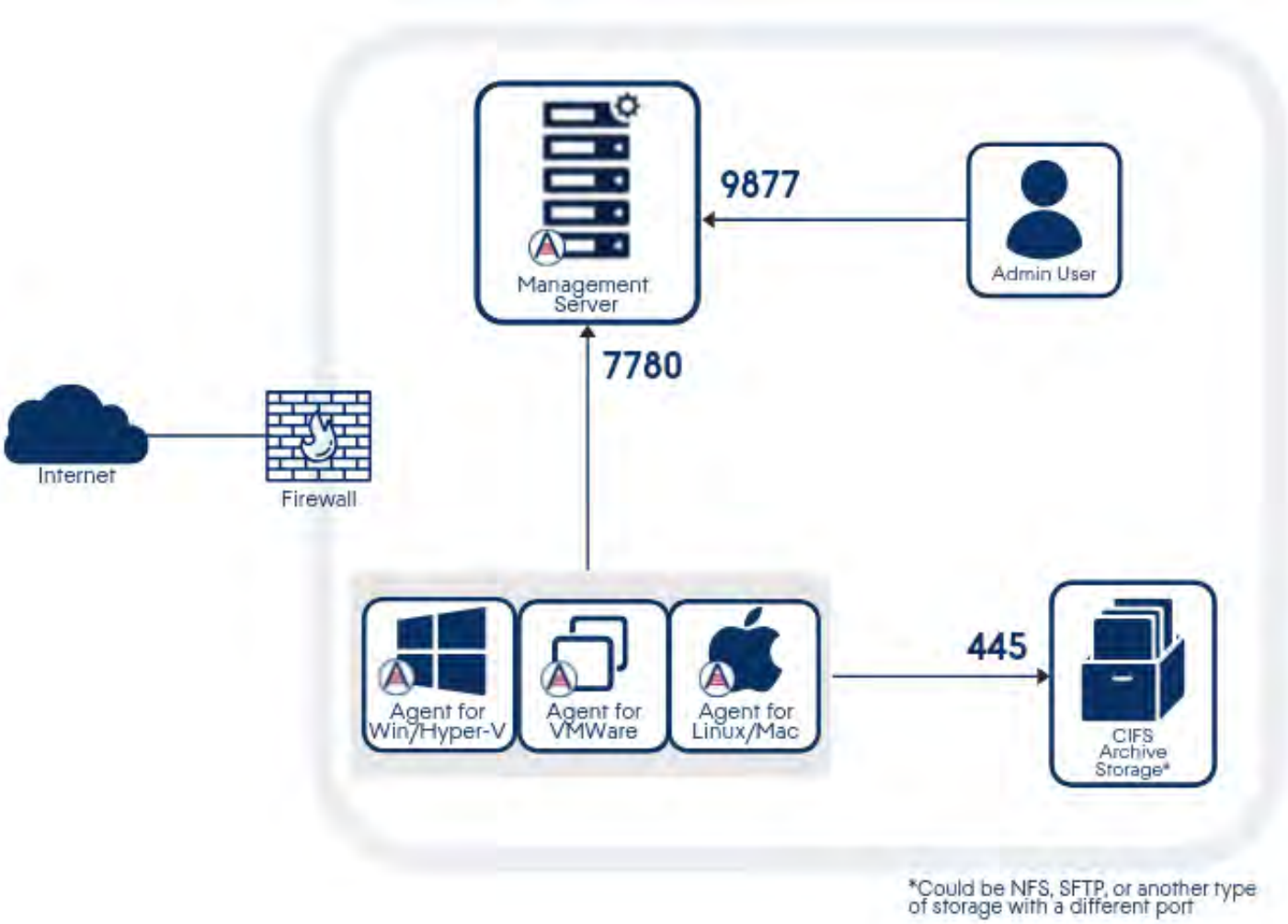
Should you have questions, please do not hesitate to contact us. Our professional services team and our 100% US-based support team are standing by to walk you through deployment options for your environment, whether you have already selected Acronis SCS for your backup needs or are still deciding.

> All ports in the below diagrams are transmission control protocol (TCP).

SCENARIO 1 – SIMPLE ISOLATED INTERNAL NETWORK

This is the most common layout for small- and medium-sized businesses (SMB), government agencies, and municipalities, as well as single office / home office (SOHO) environments. It consists of a single firewall that creates one internal zone separated from the internet.

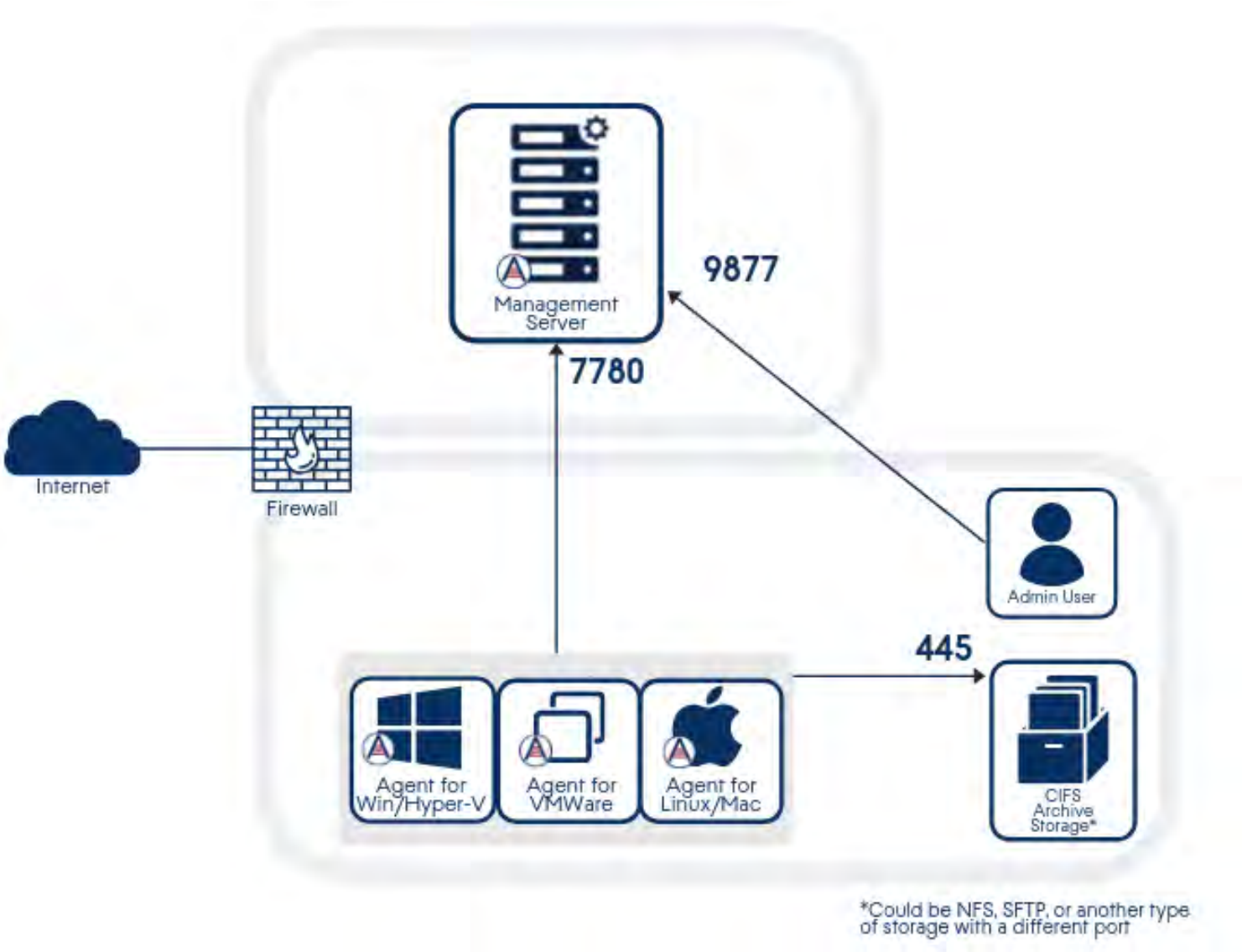
Network Firewall Rule Requirements: None, since the admin user(s), agents, management server, and archive storage are all located in the same network segment. Local firewall ports are shown below.



SCENARIO 2 – ISOLATED MANAGEMENT SEGMENT

In this environment, administrative and management access is restricted by network segmentation. This layout is most common in large enterprises, government agencies, and municipalities where dedicated IT teams manage multiple enterprise-wide systems.

Network Firewall Rule Requirements: The management server requires an open inbound port 7780 from all agents (endpoints that have the Acronis SCS backup software installed) and an open inbound port 9877 from any computer where the admin(s) uses a browser to connect to and log into the management server.

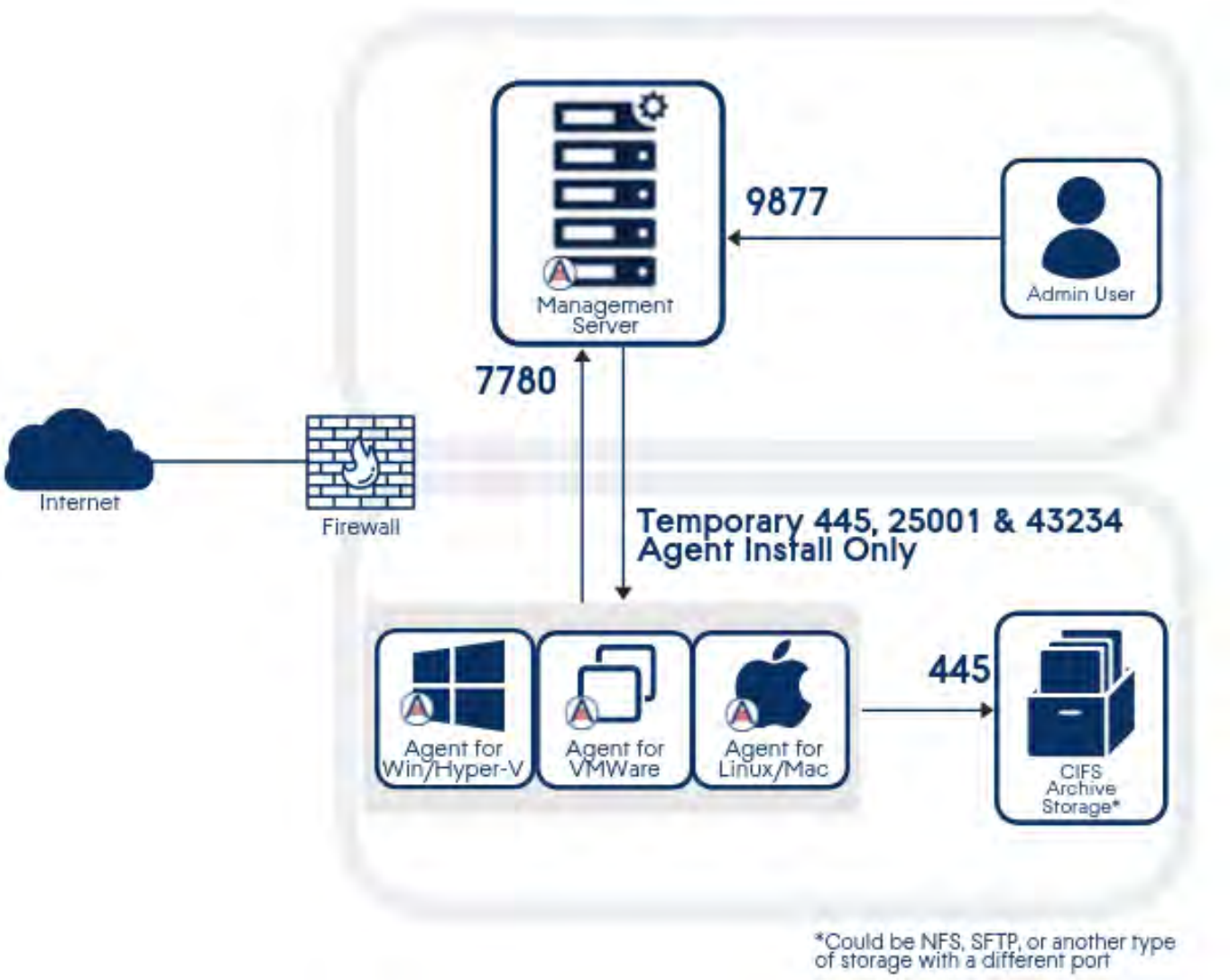


SCENARIO 3 – SENSITIVE DATA SEGMENTATION (PCI/HIPAA/CUI)

This environment uses network segmentation as a control to limit access to sensitive data. Acronis SCS's backup solutions are ideal in these scenarios, because our unique management protocol does not require data to be processed by the management server. Only our agent software needs access to the archive storage. This can greatly reduce the scope and attack surface of your protected environment, because the management server and the admin user(s) never need network access to create and manage backup plans and perform restorations.

Network Firewall Rule Requirements: All agents (endpoints that have the Acronis SCS backup software installed) require an open outbound port 7780 to the management server.

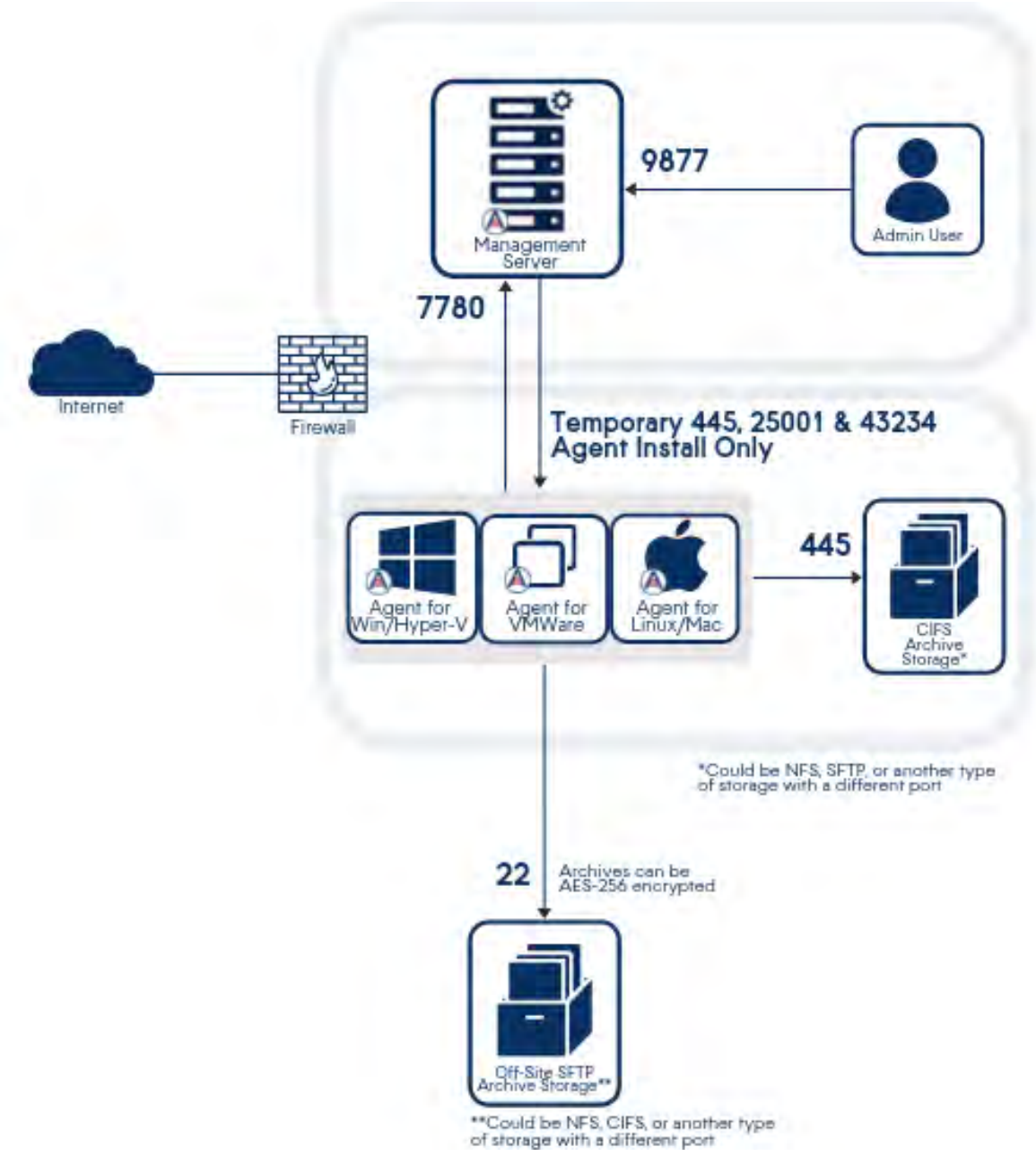
The above requirement assumes the backup software is already installed on your sensitive systems. If you must first push and install the software, open a temporary flow from the management server to all the agent install locations via the agents' inbound ports 445, 25001, and 43234 (shown below). Close these ports once the software is installed and registered.



SCENARIO 4 – SENSITIVE DATA SEGMENTATION (PCI/HIPAA/CUI) WITH OFF-SITE REDUNDANCY

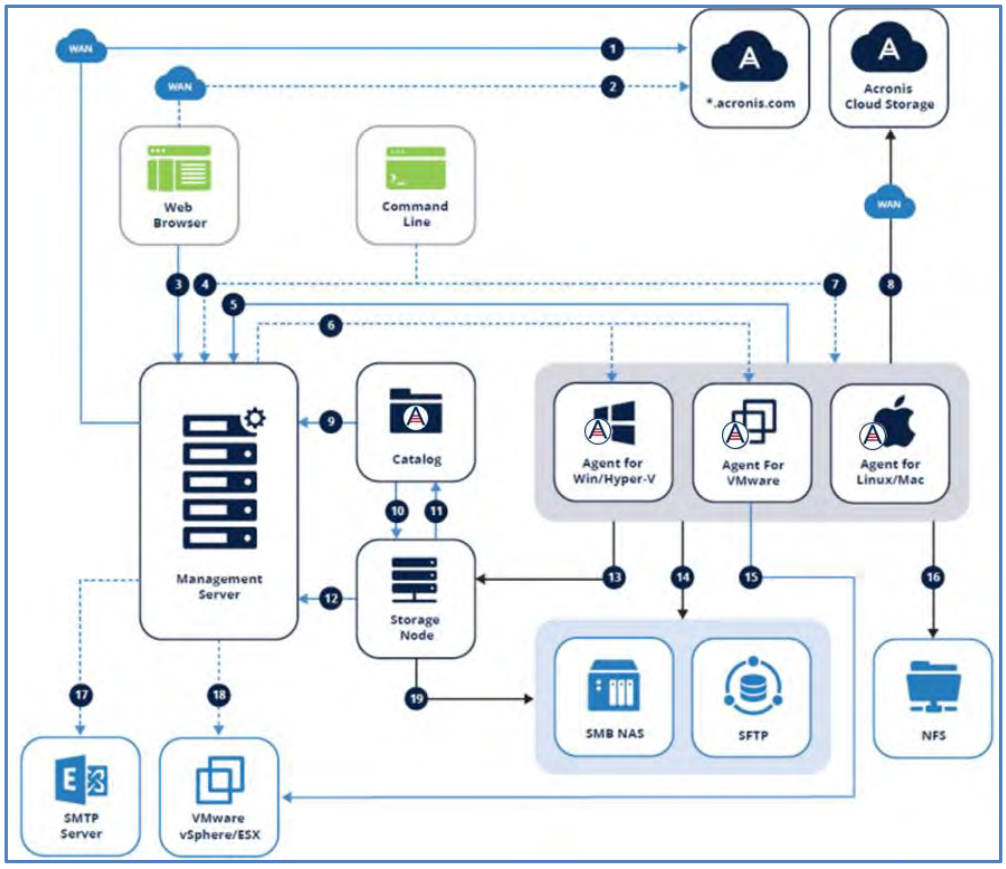
In this scenario, there is strict segmentation to protect sensitive data, as in scenario 3, with the addition of off-site storage archives for catastrophic recovery purposes. As an additional feature, these off-site archives can be AES-256 encrypted. Acronis SCS uses public/private keys with passphrase to encrypt these archives, and the passphrase you create is never stored anywhere (*only* you know it), and it can never be reverse-engineered – not by us and not by your admin(s).

Network Firewall Rule Requirements: All agents (endpoints that have the Acronis SCS backup software installed) require outbound port 7780 to the management server and outbound port 22 to the off-site SFTP server.

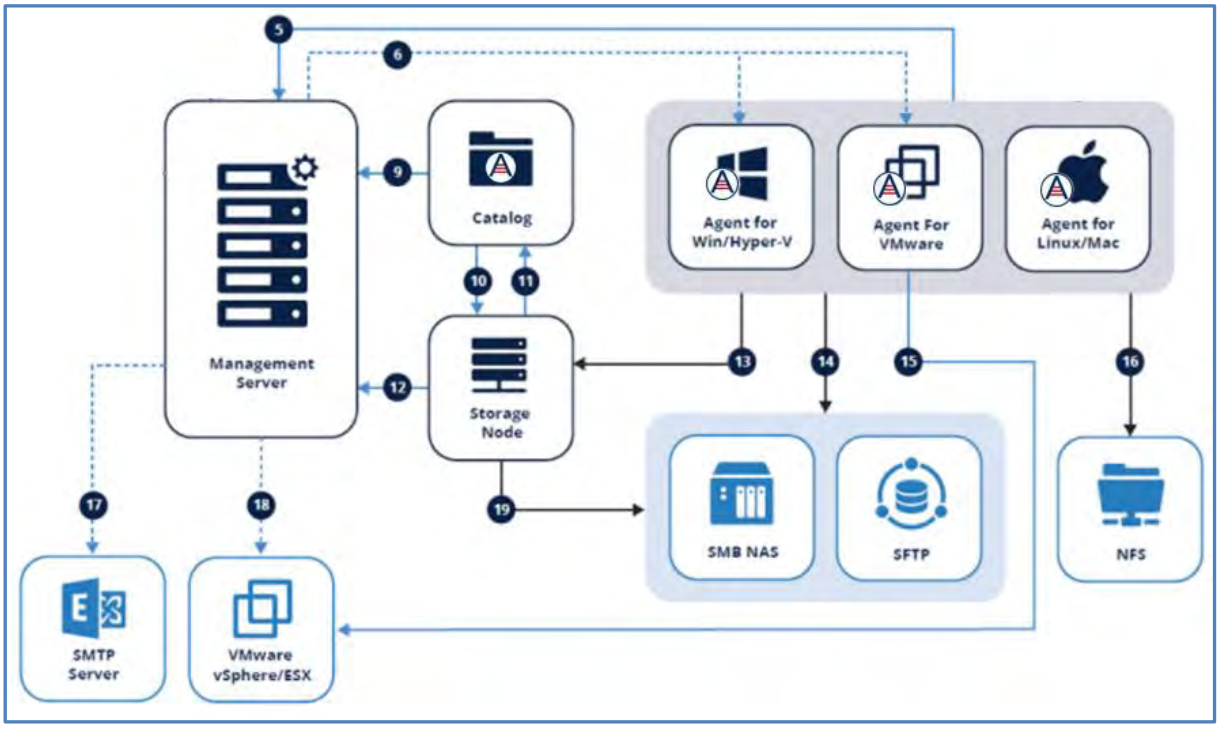


APPENDIX A – COMPLETE NETWORK DIAGRAM AND PORTS

Acronis SCS Backup 12.5



Acronis SCS Hardened Backup



Legend

The arrow direction shows which component initiates the connection. Note that all ports are TCP unless otherwise specified.

1. Download installation components: 80 to dl.acronis.com	12. - Manage ASN: 7780 ZMQ - Register ASN and manage tasks: TCP 9877
2. Sync subscription licenses: 443 to account.acronis.com	13. Backup to managed location: 9876,9852
3. Manage Environment: 9877	14. - SMB: UDP 137, UDP 138 and TCP 139, TCP 445 - SFTP: 22 (default, can vary)
4. Access via remote CL (acrocmd, acropsh): 9851	15. Create VM backups: 443, 902
5. - Register Agent: 9877* - Manage Agent: 7780 ZMQ - Sync licenses: 9877	16. NFS: TCP, UDP 111 and 2049
6. Remote installation: **U1 and earlier:** 445, 25001, 9876 **U2+:** 445, 25001, 43234	17. Send reports and emails: SMTP (25, 465, 587, etc)
7. Access via remote CL (acrocmd, acropsh): 9850	18. Deploy Appliance: 443, 902
8. Create backups to Acronis cloud storage: 443, 8443, 44445, 5060	19. - SMB: UDP 137, UDP 138 and TCP 139, TCP 445 - SFTP: 22 (default, can vary)
9. Browse and search backups: 9877	
10. Index backups: 9876	
11. Receive catalog metadata: 9200