SILVERFORT

Securing Networking Devices with Silverfort's MFA Protection

The importance of having robust protection for networking devices in today's security landscape cannot be overstated. Networking devices including routers, switches, and firewalls are attractive targets for malicious actors seeking to exploit them, disrupt services, or gain unauthorized access to sensitive resources.

Consequently, the need to safeguard networking devices has become a paramount concern, not only for the integrity and availability of data and services but also for overall organizational security. To address these challenges, Silverfort provides a multi-factor authentication (MFA) protection layer for all networking gear.

Protecting Networking Devices with RADIUS Authentication

The typical networking device authenticates to RADIUS servers, which are supported by Silverfort. With Silverfort, customers who use RADIUS can easily deploy MFA protection across their organization through seamless integrations with modern MFA push prompts and MFA tokens like Yubikey, FIDO2-compliant devices and more. RADIUS authentication plays a vital role in securing networking devices as it enables administrators to control user access and monitor usage while maintaining a centralized and efficient authentication process.

With Silverfort's MFA protection capabilities, you can significantly strengthen your RADIUS authentication process to secure the networking devices implemented across your environment. Simply knowing the credentials of the users connecting to these devices with RADIUS authentication is not enough, but adding MFA and authentication policies to the users who are accessing these devices is where Silverfort provides a vital, proactive layer of protection to networking devices.

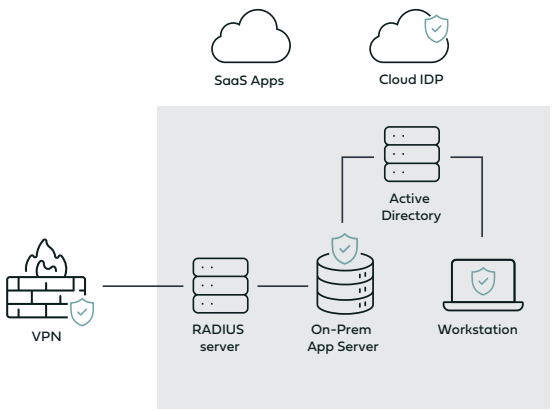
How Silverfort Supports RADIUS Authentications

Silverfort supports RADIUS authentication in two different ways. First, if you have a RADIUS server that is integrated with Active Directory, Silverfort will see all RADIUS authentications and you will have complete visibility into every access request to your networking devices.

Second, if you don't have a RADIUS server implemented, the Silverfort node replaces the need for one and becomes the RADIUS server. By configuring Silverfort as the RADIUS server for the protected clients and creating a Silverfort policy for all RADIUS authentications, you can apply RADIUS authentication requests to the configured RADIUS clients. Silverfort also provides a RADIUS OTP token configuration that allows a client machine (using PAP protocol) to send a password and the OTP code as one string so a user can initiate MFA.

Standard MFA

Standard MFA solutions typically only support certain types of resources: cloud apps, on-prem machines, remote connections, etc., resulting in operational complexities and an inconsistent user experience.



Silverfort MFA

Silverfort natively integrates with all the IdPs in the environment – on-prem, cloud, local apps, **RADIUS**, and others – to cover all MFA needs in a single solution.