HUGHES
An EchoStar Company

BROCHURE

Secure Remote Access

Strong One-Time Passcodes Through Hard or Soft Tokens

For many enterprises, user authentication tokens—which generate random and swift changing passwords—are the safest and most secure way for remote users to access a network. With two different methods for accessing this password, users now have options.

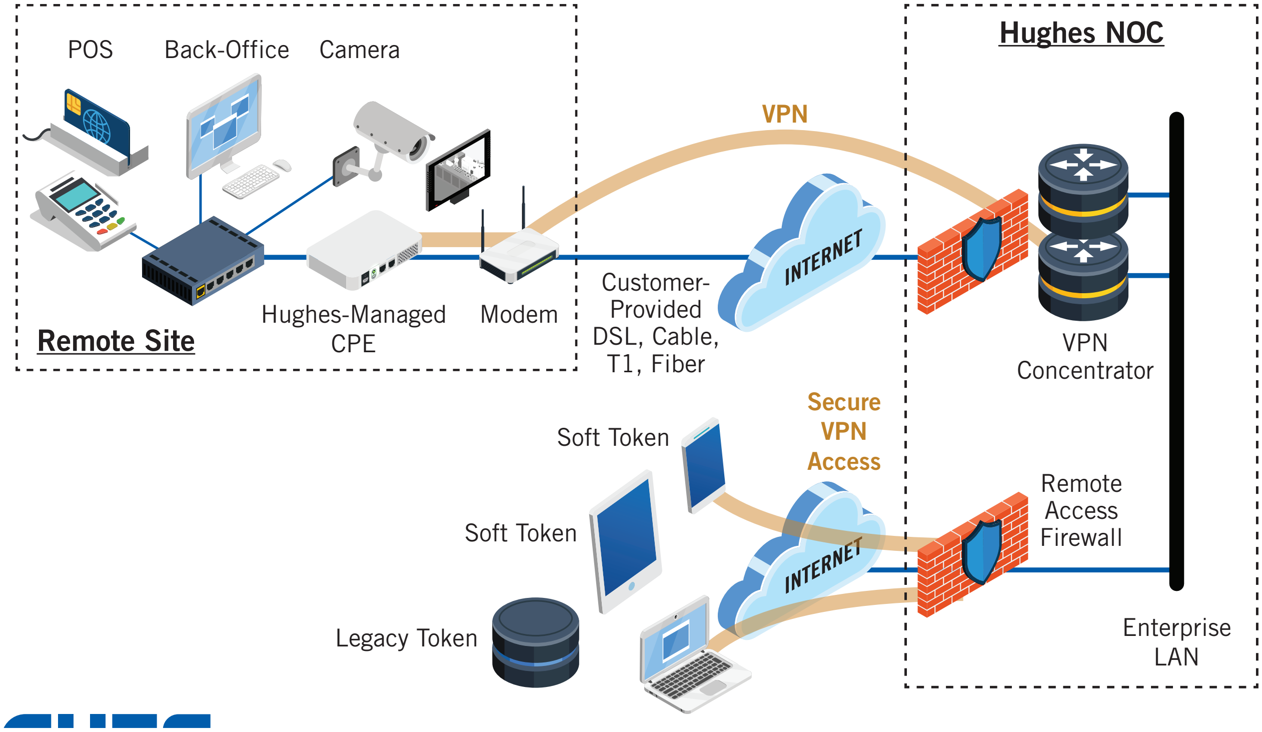
Hard Token: Traditional Two-factor Authentication

The traditional means of authenticating someone is to verify his or her preregistered username and password. This authentication scheme relies on the use of a physical token that must be in the user's possession when it generates a one-time passcode (OTP) for log-in. By utilizing this authentication method, a higher level of security can be achieved; thieves are no longer able to steal passwords written on scraps of paper or hack weak passwords online.

Soft Token: An Easier, More Convenient Approach to Tokens

Now, rather than having to rely on a hardware token, which can get lost or stolen, the newest method of token generation is through a mobile device. It enables a user to generate a strong, random, and time-sensitive one-time passcode at time of log-in, using a token generator app on a smartphone or tablet.

Hughes offers this far easier and more convenient way for enterprises like yours to authenticate users and provide secure remote access through an app. The app, which can be downloaded by users, generates strong one-time passcodes and provides access to a self-service portal for ease of password reset. For your employees, it's more manageable, more convenient, and more mobile. For your organization, it's a simple-to-implement solution that enables you to protect the network, reduce risks, safeguard data and intellectual property, streamline operational costs, and better support a remote workforce.



HUGHES
An EchoStar Company

11717 Exploration Lane
Germantown, MD 20876 USA

H56239 AUG 20