Reducing Identity Risk for VPN Access

Are Your Users Who They Say They Are?

For years, organizations have set up network perimeters to keep the bad guys (criminals) out and let the good guys (employees) in. Virtual Private Networks (VPNs) offered a safe remote connection for "good guy" access from unsecured networks to corporate systems, applications, and data that they needed in order to do their jobs.

But today's rapidly growing mobile workforce and open business environment are expanding the requirement for remote access beyond employees to include contractors, vendors, customers, audit teams, and partners. In order to do business, stay competitive, and maintain agility, modern companies are opening their networks to this broader user base.

In doing so, boundaries blur – and traditional perimeters dissolve. The emergence of identity as the new perimeter – as well as a major threat vector – places a premium on ensuring that your remote access is secure.

VPNs and firewalls continue to be the stalwarts for critical and secure anywhere-anytime remote access. But in the current business environment, it takes a little more effort to ensure that users *really are* who they say they are. If you recently purchased, implemented, or already have a VPN or firewall in place, here are a few things to consider:

Username and Passwords Are Not Enough

According to the 2016 Verizon Data Breach Investigations Report, "63% of confirmed data breaches involved leveraging weak/default/stolen passwords." Username and passwords simply don't provide enough protection – and expose your systems and data to cyber threats. What to do? Add strong authentication. Two-factor authentication (2FA) methods require users to have two forms of identification – something they know (e.g., username and password) and something they have (e.g., a hardware token) – in order to achieve VPN access. Multi-factor authentication (MFA) tools extend this concept with a third identifier – something the users are (e.g., unique physical or behavioral characteristics) – and provide convenient security for your remote users with a variety of authentication options such as push notification and biometric (e.g., fingerprint).

Assuring Identity and Appropriate Access

Depending on your specific industry, 2FA and MFA for remote access may be a requirement. Knowing that your users really are who they say they are, though, is critical for organizations in

any industry. In addition, it's important to ensure that users have the appropriate access to your systems and applications – and that this access is managed consistently in order to meet compliance and governance demands. A security solution that provides convenient and strong authenticated access based on risk analysis and contextual awareness, and that automates processes to manage which systems and resources users can access is crucial to securing your remote gateways.

Setting the Standard

The variety of types of users introduces other variables. A vendor's security standards, for instance, may not be the same as yours. In its March 2016 research report, the Ponemon Institute reported "a lack of confidence in third parties' data safeguards, security policies and procedures." While you have no control over other organizations' policies or the behavior of external users, 2FA or MFA allows you to enforce security standards that grant vital remote VPN access to your corporate systems and resources to authorized users only.

Securing Credentials

The high-profile 2013 Target data breach further underscores the importance of securing your network access to third-parties. Stolen credentials from the retailer's subcontracted HVAC vendor led to the devastating attack on Target that resulted in the theft of the data of 70 million customers and 40 million credit/debit cards. The ability to collaborate and connect with external and geographically dispersed users is essential in our digital age. Their environments, behaviors, and devices, though, are beyond your control. One thing is certain: Ensuring the security of the remote user access to your systems IS under your control.

VPNs and firewalls continue to be effective remote access gateways. To assure that your users are who they say they are, though, you must protect access via these solutions with strong authentication.

Modern identity and access assurance solutions such as RSA SecurID® Suite provide multiple secure and convenient ways to authenticate all of your users, analyze their behavior and context, and assure that the right individuals have the right levels of access – from anywhere and any device.

The bottom line? Start with a security solution that protects your VPN access against identity threats with convenient AND secure access. Talk with an RSA security expert today. Better yet, visit RSA.COM/TRYSECURID to sign up for a free trial.