

### When Passwords are not enough...

#### The Challenge:

Secure remote access requires strong authentication, but that solution must be easy to use, simple to deploy and require little administration.

#### The Solution:

SecureAuth protects your SSL VPN with two-way two-factor authentication, that not only validates the user's identity but insures the integrity of the connection over the Internet.

#### The Benefits:

The combination of MultiFactor SecureAuth and the Juniper Networks IVE provides the best security for your SSL VPN and is:

- easy to use, providing for self-service registration;
- simple to deploy, with the SecureAuth appliance in your DMZ;
- low administration, requiring no new user data-store or data replication;
- more secure, with automated two-way certificate based network integrity checks.



## Securing Juniper Networks SSL VPN Solutions

### SecureAuth Two-Way Two-Factor Authentication for Secure Remote Access

In today's environment remote access is essential to productivity and business continuity. Providing remote access to information and resources allows businesses to extend the investment in applications to field personell, extranet partners, contractors and remote employees.

In today's security climate passwords are not enough.

Two-factor authentication requires more than just a username and password. It requires that the person accessing the SSL VPN know something, a password, and that they have something. Traditional two-factor solutions are really password replacements, and although they may strengthen the password, they do nothing to assure the security of the network.

MultiFactor's SecureAuth leverages x509 digital certificates to provide a second identity factor, and to assure the integrity of the connection from the remote computer to the SSL VPN.

### The Challenge

The challenge for the enterprise has been to deliver a user validation system that provides the user identity to the trusting resource in a deployable and secure manner. Previous solutions have either burdened users or have proven difficult to deploy. In addition, previous solutions have not addressed modern identity theft attacks such as Man-in-The-Middle, replay, and DNS attacks. To solve these new validation issues, a solution must be able to create a verifiable bi-lateral authentication where the client and the server are authenticated.

The challenge has recently been stiffened by the explosion of Internet enabled mobile devices. Fortunately, Juniper has achieved great success in creating an SSL VPN solution that supports mobile platforms. SecureAuth, too, has been equal to the challenge by boasting the same level of security for iPhone, Windows mobile, and other mobile browsers, that it boasts for the Juniper SSL VPN.

## The Juniper Networks MultiFactor SecureAuth Solution

Combined with Juniper SSL VPN, MultiFactor Corporation's SecureAuth provides a bi-lateral authentication solution that will protect an enterprise from modern identity attacks. With a multi-platform, self-service enrollment model, SecureAuth is a solution that delivers strong security with no user friction. A typical user experience entails a user accessing a Juniper SSL VPN URL to request access. Features in the Juniper SSL VPN are engaged to require the Juniper appliance to query the client for a valid X.509v3 certificate, or the SecureAuth web-based validation routine will query the user's system for the identity. When a user does not have a valid certificate, the session is redirected to SecureAuth enrollment where the user's identity is verified and registration is completed.

During enrollment the SecureAuth appliance verifies the user's identity via a configurable authentication process. SecureAuth will read from fields in the enterprise own data store, to retrieve information that will allow the user to prove his identity (Note: SecureAuth does not store any user information and it integrates with all data stores). User validation choices include:

- Telephony one-time-registration code
- SMS/Text Message one-time-registration code
- E-mail one-time registration code
- Static PIN
- Knowledge-Based-Questions
- Help Desk Assisted

Upon user validation, SecureAuth initiates the X.509v3 private/public key creation on the client side. It is key to note that during the certificate creation process the private key never traverses the network. SecureAuth signs a PKCS #10 request via a web service hosted C.A. or a SecureAuth appliance C.A. that resides at the enterprise. In either deployment scenario, the certificate is uniquely mapped to the deploying enterprise and to the enrolling user. This certificate creation process is transparent to the user.

Once created on the client, the certificate is used for all subsequent authentications. As long as the certificate is valid, the user enters only his username and password. The X.509v3 certificate will allow for a bi-lateral authentication of the individual user and the server, and thereby thwart any Man-in-the-Middle, phishing, or network-based attack. Certificate lifetimes are configurable by the enterprise using SecureAuth's easy-to-use administrator's web-based interface. When a certificate expires, the date of expiry is identified by the validation process and the user is consequently redirected to the SecureAuth enrollment process to re-authenticate, re-enroll and create a new certificate.

## Integration with the Juniper Networks SSL VPN

SecureAuth can be integrated with the SSL VPN in two different models.

### Native Certificate Support

The Juniper SSL VPN can be configured to request client certificates from the browser. The client certificate can provide identity information to the SSL VPN and participates in securing the network session from the user's computer to the SSL VPN. This model is based on native SSL routines, and the SSL protocol.

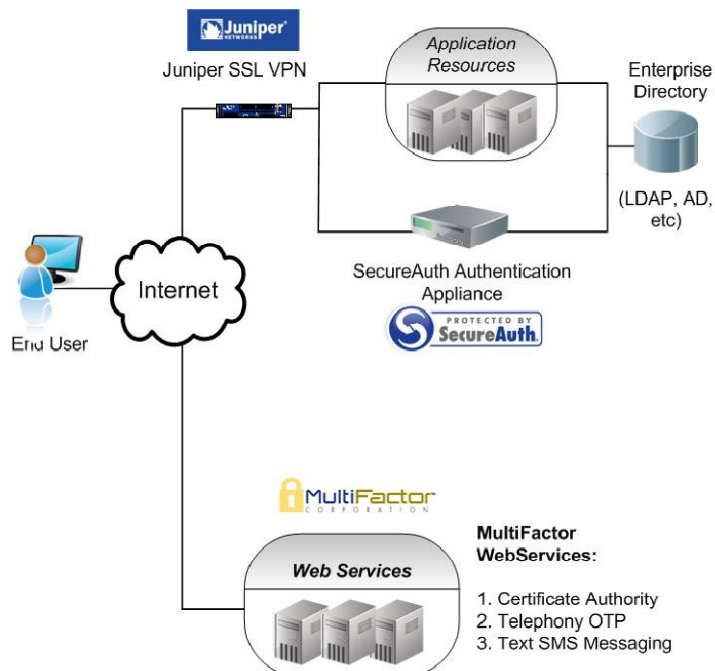
SecureAuth, when integrated in the native-certificate model, provides for the enrollment and creation of x509 digital certificates on the end-user system, leveraging the enrollment process described above. The certificate is deployed to the native keystore via ActiveX, Safari or Firefox plugins

### SecureAuth Web-Validation and Authentication

The benefit of the SecureAuth Web-Validation model is the lighter footprint, and reduced end-user friction. Instead of requiring a plugin to install certificates in the native keystore SecureAuth uses a Java applet and performs the certificate validation, network integrity checks and authentication via a web-based service. Integration is based on the Juniper SSL VPN support for SAML assertions. Once a session has been validated and authenticate a sessioning ticket is passed to the SSL VPN

### Deployment Architecture

SecureAuth is deployed in your environment as an appliance, connecting to your existing user data-store.



## Summary

The SecureAuth and Juniper SSL VPN solution is the most deployable and user-friendly solution in the market for secure remote access, providing network security that passwords and password replacements cannot achieve.

## About MultiFactor Corporation

MultiFactor Corporation is the leader in strong, simple to use, user authentication. SecureAuth is a true plug-n-play authentication mechanism that allows secure access into the enterprise network and application resources. Enabling the enterprise to cost effectively harness the true power of the network.

Please visit <http://www.multifa.com>.