

Juniper Networks SSL VPN Integration with MultiFactor SecureAuth

Simplifying X.509v3 Authentication to a Juniper SSL VPN Installation

Enterprises require secure authentication solutions for their Juniper SSL VPN deployments. The ideal solution should provide strong security by mitigating phishing, replay, man-in-the-middle, Domain Name System (DNS), and other identity theft attacks, while not burdening users or deploying enterprise administrators.

X.509v3 certificates are known to solve most security issues involved with SSL VPN authentication. The issue with certificates, however, has been the difficulty associated with enrolling users, and the bulkiness of the deployment for the enterprise. MultiFactor Corporation's SecureAuth® overcomes both of these challenges by providing a solution that features user self-service enrollment with a "drop-in" certificate service that requires no public key infrastructure (PKI) expertise.

SecureAuth supports the widest range of client devices, including Windows, Mac, Linux, iPhone, and other browser-based smart phones.

Challenge:

Provide a secure and simple-to-deploy authentication solution for the Juniper SSL VPN solution

Solution:

MultiFactor SecureAuth, an X.509v3-based solution that is simple to use and seamlessly integrates into the Juniper SSL VPN solution

Benefits:

- User self-service enrollment
- Integrated authentication/certificate enrollment
- No data store synchronization
- Flexible infrastructure models, including virtual or hardware appliance
- Supports Windows, Mac, Linux, iPhone, Windows Mobile clients, and other browser-based smart phones

The Challenge

The challenge for the enterprise has been to deliver a user validation system that provides 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, bilateral authentication where the client and the server are authenticated.

The challenge has recently become even more difficult with the explosion of Internet-enabled mobile devices. Fortunately, Juniper has achieved great success in creating an SSL VPN solution that supports mobile platforms. SecureAuth has been equal to the challenge as well by providing the same level of security for iPhone, Windows mobile, and other mobile browsers that it provides for Juniper's SSL VPN.

The Juniper Networks MultiFactor SecureAuth Solution

Combined with Juniper's SSL VPN, MultiFactor Corporation's SecureAuth provides a bilateral authentication solution that protects 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, requiring the Juniper appliance to query the client for a valid X.509v3

certificate. When a user does not have a valid certificate, the Juniper SSL VPN will redirect that user to the SecureAuth appliance and rely on SecureAuth to subsequently verify the user's identity and issue him an enrollment.

Once on the SecureAuth appliance, the user's identity is verified via a configurable authentication process. SecureAuth will read from fields in the enterprise's 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
- Short message service (SMS)/text message one-time registration code
- Email one-time registration code
- Static PIN
- Knowledge-based questions
- Help desk assisted

Once the user validates his identity using one of the listed methods, he is optionally asked to authenticate with a password that is mapped to the enterprise's data store; this ensures that the user still exists and can authenticate against the enterprise's user data store.

Upon user validation, SecureAuth initiates the X.509v3 private/public key creation on the client side. It is important 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 certificate authority (CA) or an infrastructure CA that resides at the enterprise. In either deployment scenario, the certificate is uniquely mapped to the deploying enterprise and to the enrolling user, with the certificate creation process 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 bilateral 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, web-based administration interface. When a certificate expires, the date of expiry is identified by the Juniper SSL VPN, and the user is consequently redirected to the SecureAuth appliance to re-authenticate, re-enroll, and create a new certificate.

Features and Benefits

User Self-Service Enrollment

One of SecureAuth's marquee differentiating features is the user self-service enrollment process. SecureAuth places the user's private/public keys in the native key stores without any user assistance; this eliminates the need for a support call to the enterprise or the need to educate users on certificate usage.

URL-Based Enrollment

Because the SecureAuth enrollment site is "exposed" to the enterprise as a URL, it is simply a matter of configuring the Juniper SSL VPN to set up SecureAuth as the X.509v3 enrollment site. No API or programming is required. The SecureAuth appliance simply becomes the trusted site for validating users and issuing valid certificates.

Built-In Secure Enrollment Methods

SecureAuth verifies the user's identity via a configurable authentication process. The user is validated using a choice of options that include a telephone call, SMS/text message, PIN, knowledge-based answers, or a help desk model.

Utilizes Current User Store

There is no data syncing in the SecureAuth deployment model. SecureAuth is configured to use the enterprise's data store, which can include LDAP, Active Directory, and MS/SQL.

Web Service or CA Infrastructure Model

SecureAuth hosts its own set of telephony, SMS, and certificate services. An enterprise may choose to host a SecureAuth Certificate Appliance or to use SecureAuth's Web services. Both models are secure and require minimal integration or maintenance.

Configurable Certificate Lengths

SecureAuth can be configured to deliver two types of certificates for the user:

Long Term	2 days – 10 years
Short Term	2 – 48 hours

Certificates are configured by administrators in the simple-to-use SecureAuth Web configuration tool. No PKI knowledge is required.

Solution Components

NOTE: As a prerequisite for deployment the SecureAuth solution requires any Juniper SA series appliance properly licensed for SSL VPN.

The SecureAuth solution can be deployed in two simple deployment scenarios.

1. SecureAuth Authentication Appliance and Web Service

In this scenario, a SecureAuth authentication appliance is installed at the enterprise. It consists of three primary components:

- A. An enrollment Web server
- B. Data connectors

Data connectors connect the SecureAuth appliance to the enterprise data store. An administrator may do this by using the SecureAuth Web GUI to securely connect to the enterprise data store.

- C. Web service connectors

Web Service connectors are pre-configured in the SecureAuth authentication appliance. SecureAuth uses the MultiFactor hosted Web service for:

- Certificate Authority
- SMS (text) messaging
- Telephony

2. SecureAuth Authentication Appliance and a SecureAuth Certificate Appliance

In this scenario, the SecureAuth authentication appliance is installed at the enterprise; however, in lieu of MultiFactor Corporation's Web Service for the Certificate Authority, a SecureAuth Certificate Appliance is also installed at the enterprise. The SecureAuth Certificate Appliance substitutes for the Web certificate service used for deployment scenario #1. In this second scenario, the SecureAuth Appliance makes a secure Web service call to the SecureAuth Certificate Appliance.

Illustration:

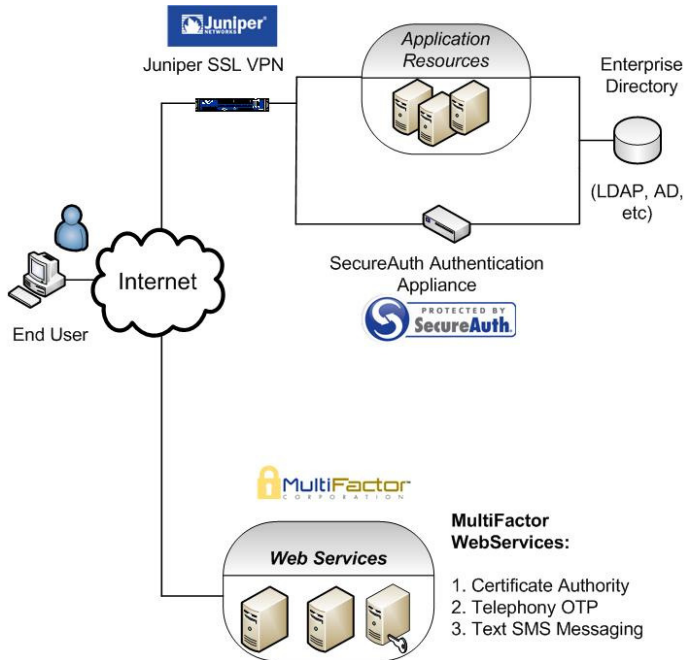


Figure 1. Scenario #1—Juniper SSL VPN and a MultiFactor SecureAuth authentication appliance (certificates issued by secure MultiFactor Web Services)

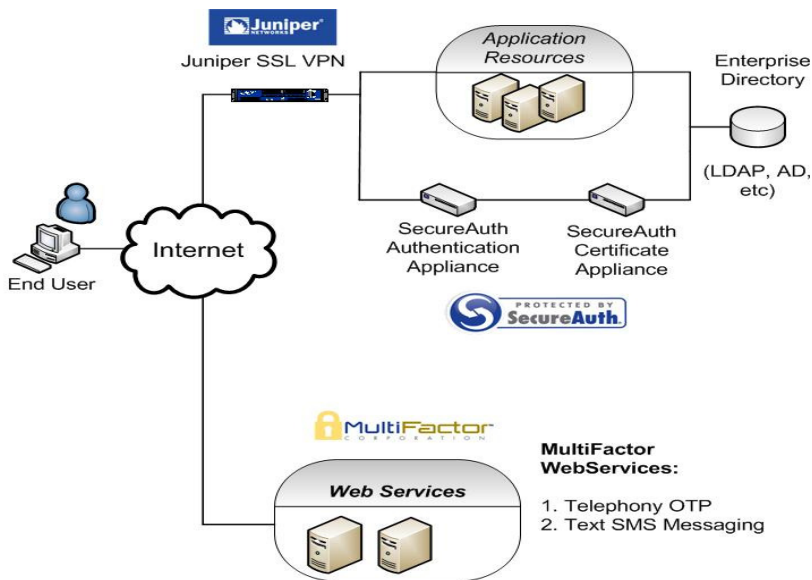


Figure 2. Scenario #2—Juniper SSL VPN and a SecureAuth authentication appliance and a SecureAuth Certificate Appliance (certificates issued by a MultiFactor SecureAuth Certificate Appliance)

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.

Next Steps

To learn more about Juniper SSL VPN integration with MultiFactor SecureAuth, please contact your Juniper Networks representative at <http://www.juniper.net> or MultiFactor Corporation at <http://multifa.com>.

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.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Copyright ©2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.