

COST-EFFECTIVE MULTIFACTOR AUTHENTICATION FOR ALL JUNIPER NETWORKS SA SERIES SSL VPN APPLIANCE USERS

Challenge

Today's security strategies incorporate multifactor authentication for secure remote access. But today's organizations need software-only, low overhead authentication solutions that don't require hardware or software provisioning.

Solution

Working with Juniper Networks SA Series SSL VPN Appliances, AdmitOne Security offers an integrated, simple and powerful solution for authenticating a user's login credentials with their keystroke dynamics – an individual's unique typing rhythm. This clientless solution can be rolled out to all SA Series users quickly.

Benefits

- Layered multifactor authentication solution using login credentials, keystroke dynamics, Device Tags, challenge response questions (CRQ), and one-time password (OTP)
- Zero footprint solution that authenticates a specific user (not just a device, shared Information, browser or location) without requiring a client
- No user hardware to purchase, manage, lose or replace

AdmitOne Security's Multifactor Authentication Software Delivers High Security for all Juniper Networks® Remote Access Users at a Dramatically Lower Cost

IT organizations are challenged constantly in keeping networks secure and applications accessible while supporting diverse computing and networking architectures for an ever-changing population of customers, suppliers, partners and employees. With these challenges come substantial security requirements for verifying identities, protecting data, ensuring privacy, proving compliance, and shielding the organization from growing internal and external fraud.

IT professionals know it is no longer practical to rely solely on the username and password to authenticate users. Highly visible and successful attacks on corporations (including phishing, pharming, spyware, as well as simple brute-force password cracks) continue to put sensitive and valuable information at risk and garner global attention. A security strategy incorporating multifactor authentication – combining something you know (a password) with something you are (a biometric) or something you have (for example, a mobile device) – for remote access is no longer a luxury item. It is mandated by responsible corporate management and government legislation.

Juniper Networks SA Series and AdmitOne Security Sentry

AdmitOne Security is the leader in delivering enterprise security software solutions for multifactor authentication using the biometric science of keystroke dynamics. Working with Juniper Networks SA Series SSL VPN Appliances, AdmitOne Security Sentry provides a simple, yet powerful combination of the user's standard login credentials (username and password), with keystroke dynamics (their unique typing rhythm) for a highly accurate and secure multifactor authentication solution, AdmitOne Security Sentry.

AdmitOne Security Sentry also offers additional software-based authentication factors, such as one-time passwords (single-use password delivered to your mobile device or email) to ensure access to every user – every time.

Deployed as a tightly integrated solution, the SA Series and AdmitOne Security Sentry provide fast, accurate and transparent multifactor authentication, without the need for expensive tokens, cards or other specialized hardware.

Using AdmitOne to monitor and authenticate remote access users, organizations can quickly and cost-effectively implement secure access, comply with regulatory requirements, and substantially reduce their fraud risk.

“A zero-footprint, strong authentication approach has the benefit of delivering the required security while completely changing the economics associated with deployment and administration.”

Scott Knights, senior IT systems security analyst
Idaho Department of Health and Welfare

Features and Benefits

Unlike existing and expensive security products, AdmitOne Security Sentry has many unique advantages.

FEATURE	BENEFITS
Zero-footprint authentication	Authenticates a specific user (not just a device, shared Information, browser or location)) without requiring additional hardware, software or certificates
Behavioral typing rhythm	Cannot be shared, lost, stolen or forgotten.
High security	The only solution to combine keystroke dynamics verification (something you are) with passwords and knowledge-based verification (something you know) or one-time passwords (something you have) for multifactor authentication.
User-friendly	Balances productivity and security without changing users' current login behavior. Simply type username and password normally.
Lowers management costs	Does not require distribution, management or replacement of a special sensor, tokens, cards or keyboards.
Lowers support costs	Lower training and procurement costs combined with integrated user self-service features lower overall support overhead.
Ubiquitous	Works anywhere there's a keyboard.

Solution Components

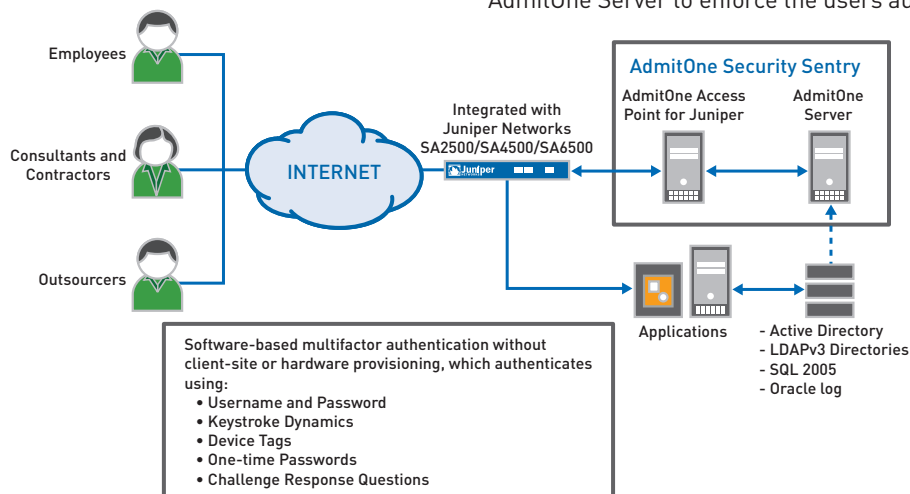
SA Series SSL VPN Appliances work with AdmitOne Security Sentry (AOSS) by providing organizations with a superior solution to monitor and authenticate remote access users.

As shown in the previous diagram, the SA Series is accessed directly from the user location via a standard Web browser and Internet connection. The SA Series intermediates the client request, performs an authentication with the AOSS, and provides further authorization and access control functions. The SA Series includes dynamic access privilege management features that consider a variety of attributes to ensure that each

user's session adheres to security policies, whether the user is a mobile employee from a managed PC or a business partner accessing an extranet.

AOSS has three components: AdmitOne Control (automatically delivered via the browser), AdmitOne Access Point for Juniper and the AdmitOne Server.

The AdmitOne Control is automatically served to the user as part of the Web session. The Control simply collects the username, password and keystroke timings (and in alternative cases, the one-time password). This information is passed through the SA Series via the AdmitOne Access Point to the AdmitOne Server to enforce the users authentication policy.



With the correct credentials and accurate keystroke dynamics, access through the SSL VPN is granted. Otherwise, access is denied. For situations in which the keystroke dynamics cannot be used, a one-time password may be deployed as a second factor of authentication.

Summary

Juniper Networks SA Series SSL VPN Appliances work with AdmitOne Security Sentry by providing organizations with a superior solution to monitor and authenticate remote access users. With our solution, organizations can mitigate the risks of remote access due to:

- Inherent password vulnerabilities: lost, stolen, shared or weak passwords
- Social engineering attacks: phishing and pharming
- Brute-force password cracking
- Man-in-the-middle and man-in-the-browser attacks

Using AdmitOne Security Sentry to monitor and authenticate remote access users, you can:

- Implement secure strong authentication quickly and cost-effectively for all users
- Provide secure strong authentication without impacting the user experience
- Comply with regulatory guidelines
- Reduce costs associated with help desk calls caused by missing bingo cards, broken tokens, or improperly configured certificates

Next Steps

To find out more about our unique solution, please contact your local Juniper partner.

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.

About AdmitOne Security

AdmitOne Security, located in Issaquah, Washington, is a venture-backed software company providing risk-based authentication solutions for preventing fraudulent use of digital identities. The AdmitOne Security Sentry is a unified platform that reduces enterprise risk by linking a right user to the right digital identity through a simple, yet powerful, combination of the standard logon credentials and risk assessment of additional in-band factors. Sentry's ability to verify users through keystroke dynamics provides industry-leading usability and protection compared to other risk-based solutions. AdmitOne's zero-footprint server-based solution is accurate, secure, scalable to millions of users and immediately deployable across the enterprise and the Internet without changing user procedures. AdmitOne is currently delivering risk-based authentication for organizations in a variety of industries, including: financial, SaaS providers, government, healthcare, manufacturing, legal and automotive. To learn more, visit our website or contact us at www.admitonesecurity.com or call (425) 649-1100.

AdmitOne Security® is a registered trademark of AdmitOne Security, Inc. All other trademarks and registered trademarks are the property of their respective owners.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, 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.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

