

# THE JUNIPER NETWORKS-SKYRECON SECURITY SOLUTION

## Delivering End-to-End Unified Network and System Security

### Challenge

With the number of security breaches being reported continuing to rise on a global basis, controlling and ensuring proper access to critical business systems and sensitive business data has become mandatory.

### Solution

With Juniper Networks and SkyRecon, organizations can ensure secure and manageable access to critical business systems, applications, and data via secured endpoints that are constantly protected from attack, theft, and misuse.

### Benefits

- Protect sensitive business data from being accessed by unauthorized people and applications
- Protect critical business systems from compromise by rogue and unprotected endpoints
- Endpoint system and data protection and access control on and off the internal network
- Dynamically control endpoint security policy in support of IT operations and internal/regulatory requirements

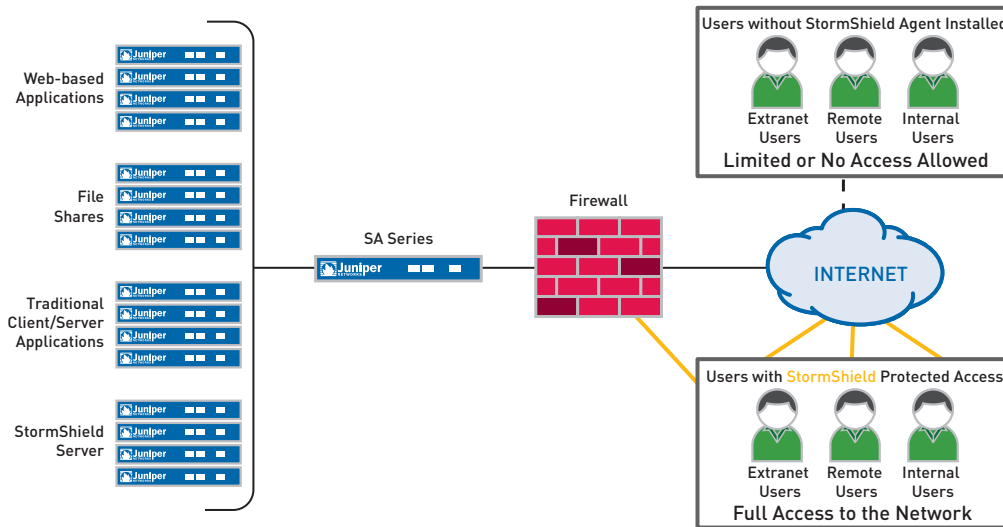
As organizations continue to extend their business operations to support an increasingly mobile workforce and expanding external partnerships, they look for remote access solutions that can support their complex business requirements by protecting their mobile workers, internal network and sensitive business data, while reducing operational costs and enabling policy compliance. Leveraging breakthroughs in sophisticated access methods and multi-layered endpoint security solutions from Juniper Networks® and SkyRecon Systems, organizations can now provide secure and manageable access to corporate applications and sensitive business data, while ensuring that the systems accessing these applications and data are protected from attack, theft and misuse.

### The Challenge

Organizations are becoming very much aware that the once solid walls built around their information systems and sensitive business data are quickly dissolving, mainly because of the irreversible trends towards increased mobile computing and Internet connectivity. Organizations are tasked with making their internal corporate assets remotely available to traveling employees, partners, suppliers and vendors. The challenge comes in striking the right balance between enabling remote access and securing the systems, networks, applications and data that ultimately enable remote business operations.

Increasingly sophisticated security threats covertly target each of these information system layers, taking direct aim at the most vulnerable layer—the endpoints. Due to the large numbers of endpoint devices, a significant portion of which remain remote and unmanaged, organizations find it extremely difficult to ensure authorized and secure access to critical and sensitive business systems and data. The time has come for Information Technology operations and Information Security operations to collaborate, bringing together best practices and technologies that integrate and work together to enable end-to-end availability and protection for all layers of the business information systems infrastructure.





## The Juniper Networks SkyRecon Security Solution

SkyRecon's StormShield™ is the industry's first integrated endpoint security product to provide single-agent protection for endpoint operating systems, applications and sensitive data. StormShield protects your business from the real threats of data leakage, data theft, system misuse, network compromise and zero-day attacks by integrating with your Juniper Networks SA Series SSL VPN Appliances.

StormShield provides real-time defense against attack and end user social engineering through the integration of device control, data encryption, application control, intrusion prevention, system firewall, anti-virus/anti-spyware, network access control (NAC) via the Juniper Networks Unified Access Control offering, and secure client access via the SA Series. StormShield's multi-layered approach provides the most comprehensive set of

protections available as a single, lightweight agent, providing complete protection without the need for signatures or rule updates. StormShield is the only solution to offer integrated device control and secure file encryption to ensure that your sensitive business data stays in the hands of the business.

The SA Series leads the SSL VPN market with a complete range of remote access appliances to meet the needs of companies of all sizes. SA Series SSL VPN Appliances use SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for client-software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. SA Series appliances combine the overall benefit of a lower total cost of ownership over traditional IPsec client solutions with unique end-to-end security features. Enhanced remote access methods enable the enterprise to provision access by purpose for virtually any resource, including those that are jitter or latency sensitive.

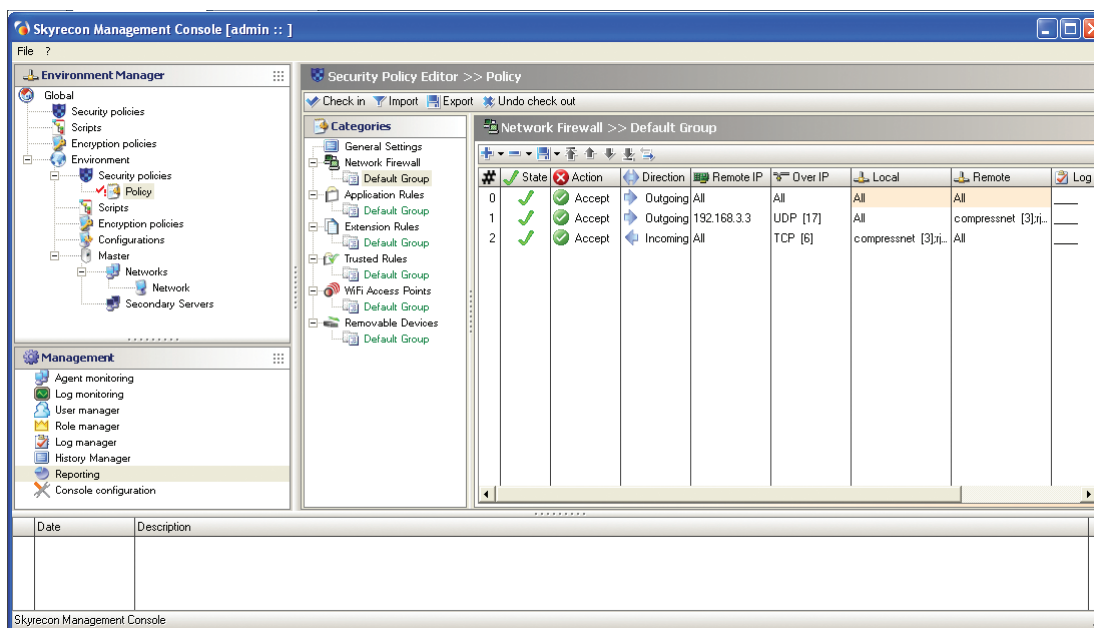


Figure 1: SkyRecon Management Console

The SA Series verifies and ensures that endpoint devices meet corporate security policy requirements before granting access, remediating the endpoint security implementation and quarantining users when necessary. Through the Trusted Network Connect (TNC), customers can leverage their existing SkyRecon StormShield implementations to utilize their current security policies for remote users and mobile endpoints, delivering seamless end-to-end network and application security policy management.

### 360° Protection for Systems, Applications and Data

SkyRecon's StormShield Unified Endpoint Protection and Juniper Networks SA Series SSL VPN Appliances work together to protect both the endpoints and the network from unauthorized access to, and compromise of critical business systems, applications and sensitive business data. Endpoints utilizing StormShield are protected from intrusions, virus and malware attacks, and the compromise of data residing on the host. Networks that use the SA Series are protected from unauthenticated connections and denial of service (DoS) attacks. Sensitive business data is protected through integrated layers of host intrusion prevention, application control, content encryption, device control, secure file erasure, and endpoint cache cleaning upon closure of the network session.

### Features and Benefits

- **Continuous Endpoint Protection:** The Juniper Networks SkyRecon Security solution ensures the endpoints are protected, maintaining protection as the endpoints move in and out of the protected perimeter of the internal network. The solution protects businesses from the real threats of data leakage, data theft, system misuse, unauthorized access, and zero-day attacks. A single, lightweight security agent delivers multiple protection layers that work together to protect both the system and the data residing at the endpoint. The integrated StormShield services include device control, file-based content encryption, application control, host-based intrusion prevention (HIPS) and firewall, anti-virus and anti-spyware protection, wireless security, and network access control (NAC).
- **Secure Network Access:** The SA Series ensures that endpoints are both free from compromise and compliant with endpoint IT security policy prior to being granted access to the internal network. While providing integrated protection against attack, SkyRecon's StormShield endpoint security solution ensures that endpoints are properly protected

in support of the defined endpoint security policy. The combined solution protects sensitive data from accidental or malicious removal and misuse through policy-based control over removable devices, secure session settings, and secure content encryption enforcement. Multiple security policies can be defined to bring the same level of protection for the internal network to mobile users regardless of their connection through the VPN, dynamically applying the appropriate policies.

- **Unified Policy Enforcement:** The combined Juniper Networks SkyRecon Security solution delivers dynamic policy management designed to help organizations find the right balance between business, IT, and security operational requirements. This balance enables collaboration between these groups, ensuring consistency and efficiency between the different operational processes. With the centralized management and reporting tools, organizations can provide proof that the required policies have been applied to their laptops, desktops, and servers. The policies can be defined to provide varying levels of protection based on the state of the endpoint device as well as the network location of the endpoint.

### Solution Components

- Juniper Networks SA2500, SA4500, SA6500 SSL VPN Appliances
- StormShield Unified Endpoint Protection (version 4.8 and greater)

### Summary—Secure Access Coupled with Comprehensive Endpoint Security

Unprotected endpoints connecting to the internal network can lead to severe business disruption and the potential for data loss or theft. Preventing this risk demands a proactive endpoint security solution and a flexible, secure access solution that combines user identity, device security and health state, along with location information for session-specific access policy by user. With the SA Series SSL VPN Appliances and SkyRecon's StormShield solutions, your network is safe because your endpoints and networking access channels are.

### Next Steps

To learn more about the StormShield/SSL VPN solution, please email [sslvpn@skyrecon.com](mailto:sslvpn@skyrecon.com) or visit us online at [www.skyrecon.com/juniper](http://www.skyrecon.com/juniper).

## About SkyRecon Systems

SkyRecon® Systems is a premier global provider of endpoint security solutions, delivering the industry's first unified endpoint protection for applications, the operating system and sensitive data. SkyRecon's StormShield™ meets the market's current and future requirements for protecting their networked and mobile PCs through the most comprehensive system and data protection available. Additional information can be found at [www.SkyRecon.com](http://www.SkyRecon.com).

## 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](http://www.juniper.net).



Tel North: 0151 2031400 Tel South: 0118 9071600  
Email: [info@castleforce.com](mailto:info@castleforce.com) Web: [www.castleforce.com](http://www.castleforce.com)

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.