

Solution Brief

Coordinated Threat Control

Juniper Secure Access
SSL VPN and
IDP Intrusion Prevention

Overview

Today's IT departments have increasing demands for providing secure remote access for employees, partners and customers. The proliferation of users along with the diversity of users, devices, and networks are only a part of the challenge. The escalating volume and sophistication of threats from intentional and unintentional attacks contribute to the challenges for extended enterprise access.

Situation

According to the 2005 FBI Computer Crime Survey, a common theme of frustration existed within IT departments with the nonstop barrage of viruses, Trojans, worms, and spyware. The survey stated that there were over twice as many unauthorized access incidents coming from outside the organization than there were from within. The survey specifically underlined the importance of Intrusion Prevention/Detection Systems as well as firewalls, logs, password complexity, and other technology and physical security measures to address the rapid growth of threats to any enterprise.

The increased need for remote access for the extended enterprise of employees, partners, and customers must be balanced with steps to ensure valuable resources and assets are protected from intentional or unintentional attacks. Granular access capabilities and endpoint security technologies provide the ability for IT to control access to applications and resources. However, while restricting access to only what a user requires is critical, it does not prevent attacks that can come from either unintentional

or malicious authenticated users. Some examples include a disgruntled employee/partner or a hacker who has compromised the authentication credentials of a user. Another example is malicious code (e.g. spyware) that has not been intercepted or discovered by endpoint security policies. In addition, sometimes practical considerations, such as restrictions as to what partners will allow a company to download to their endpoints, reduce the ability of administrators to utilize endpoint security technologies, further limiting an administrator's security tools.

A common way of adding security to a remote access deployment is to utilize Intrusion Prevention and Detection technologies. However, deploying IPS behind a SSL VPN can be limiting. When malicious traffic is detected, it can be difficult to correlate the malicious tunneled traffic to a specific user and sometimes impossible to identify a user with intermediated traffic. However, the identification of the user and the source of the malicious traffic are key in maintaining a secure network for the extended enterprise. A valid user whose remote access device may have been compromised must be notified and directed to "clean" their device of any malware. A malicious user on the other hand, must have their access blocked to prevent further network attacks. Containment and restricting any further access is imperative to safeguard all resources.

The challenge is for enterprises to secure and assure each and every session, so that they can deliver high end user productivity while protecting information assets.

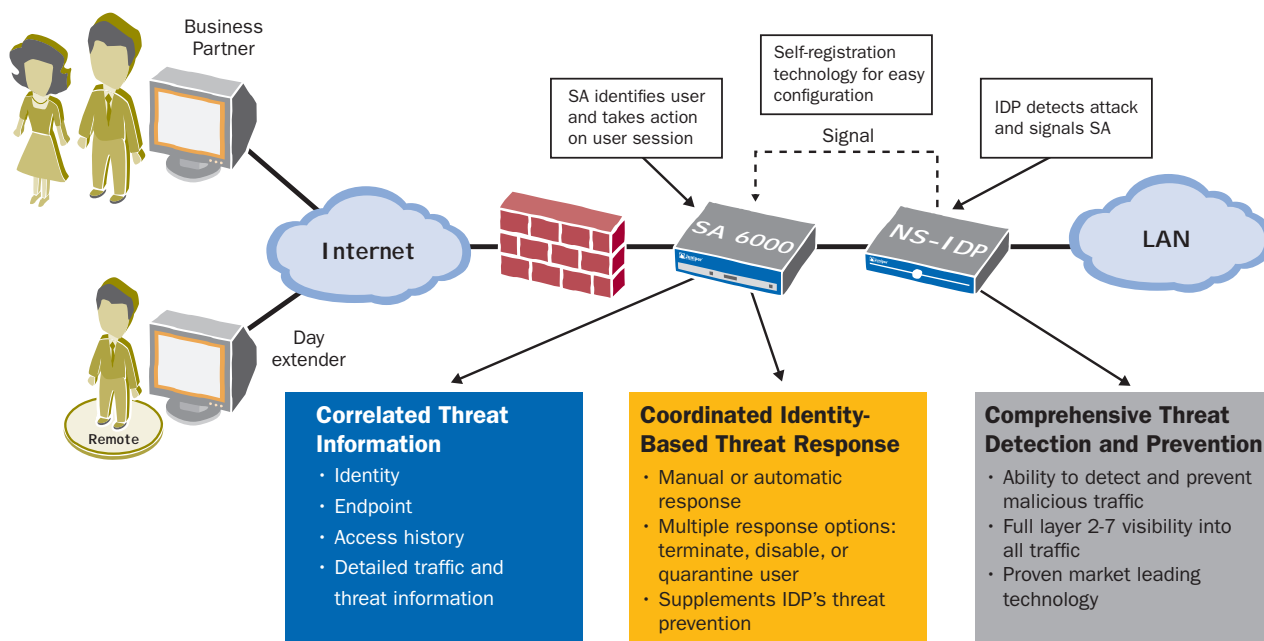


Diagram 1: Juniper Networks Coordinated Threat Control

Solution

Juniper's Coordinated Threat Control provides a solution for overcoming the challenge of balancing extranet access – for full access remote employees and partners – to critical applications while maintaining a strong security posture around the enterprise's critical assets.

Coordinated threat control technology enables Juniper's Secure Access SSL VPN and IDP Intrusion Detection and Prevention appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP to effectively identify, stop, and remediate both network and application-level threats within remote access traffic. With this technology, when IDP detects a threat or any traffic that breaks an administrator-configured rule, it signals the Secure Access SSL VPN appliance. Secure Access uses the information from IDP to identify the user session that is the source of undesired traffic.

Utilizing this information, Secure Access is able to take actions on the endpoint including: terminating the user session, disabling the user's account or mapping the user into a quarantine role. Administrators can configure the quarantine role so that they can provide users with a lower level of access to resources and inform the user of why they have been quarantined and what they should do in order to remove themselves from the quarantined role. They could also execute additional endpoint security checks or download additional endpoint protection software. Secure Access allows Administrators to take action on user sessions either manually by selecting an active user session and executing the desired action, or automatically by creating policies that will execute the desired actions as soon as a signal that matches the policy criteria is received from IDP. With this new functionality, the combined Secure Access and IDP solution allows Administrators to take action by not only blocking attacks before they reach their targets, but also by taking coordinated action against the endpoint that is the source of the attack.

Customer Value

Looking across the requirements of the extended access, it becomes apparent that Coordinated Threat Control provides unique benefits for different use cases:

Full network access:

In this scenario a user has been granted full network access. With this unfettered access comes the concern that any malware on the user's machine will also have unlimited access to the high-value assets.

In this use case, Coordinated Threat Control provides the administrator with the ability to:

- Detect and drop malicious application layer traffic (ex. worms, Trojans, spyware, keyloggers et al.)
- Control application usage on the endpoint (ex. IM chat clients, peer-to-peer programs)
- Identify source of malicious traffic, unapproved application user and take action on source (ex. disabling/quarantining accounts)
- Log detailed endpoint, user, network and application layer traffic information for security event mitigation, auditing and compliance

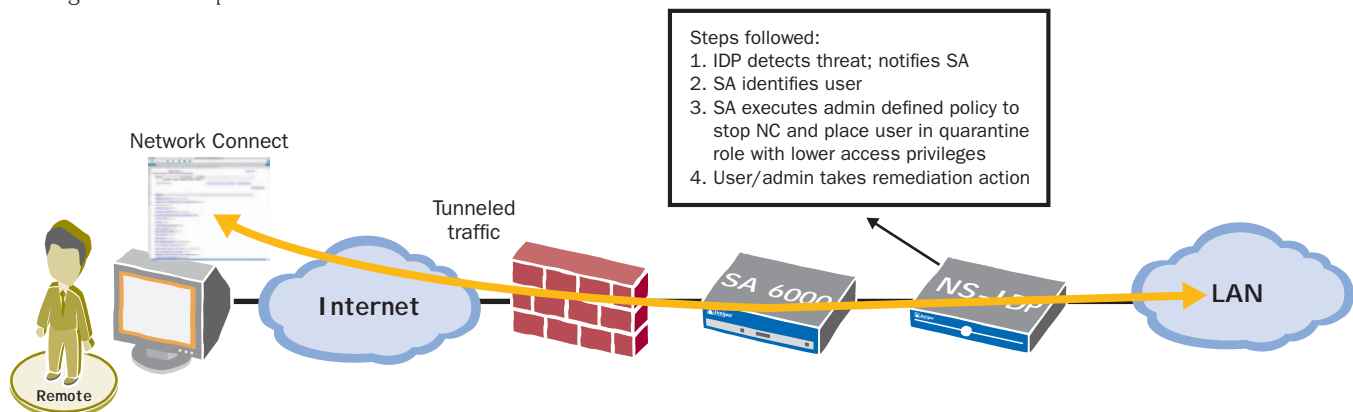


Diagram 2: Coordinated Threat Control for Full Network Access

Partner access:

In this scenario, a business partner has been given access to certain resources on the enterprises network. Since there is little control over the incoming user and her machine, the exposure to attacks is quite high.

In this use case, Coordinated Threat Control provides the administrator with the ability to:

- Only provision access to required applications (“provision by purpose”)
- Detect and drop malicious application layer traffic
- Identify source of malicious traffic and take action on source even when SSL VPN is acting as a proxy
- Log detailed endpoint, user, network and application layer traffic information for security event mitigation, auditing and compliance

Conclusion

With Coordinated Threat Control, Juniper Networks provides enterprises the ability to deploy best-in-class access and threat prevention technologies in a seamless solution that works to provide secure and assured access. With this solution enterprises can continue to service the ever-expanding need for anywhere, anytime access to information with the confidence that their security posture remains uncompromised.

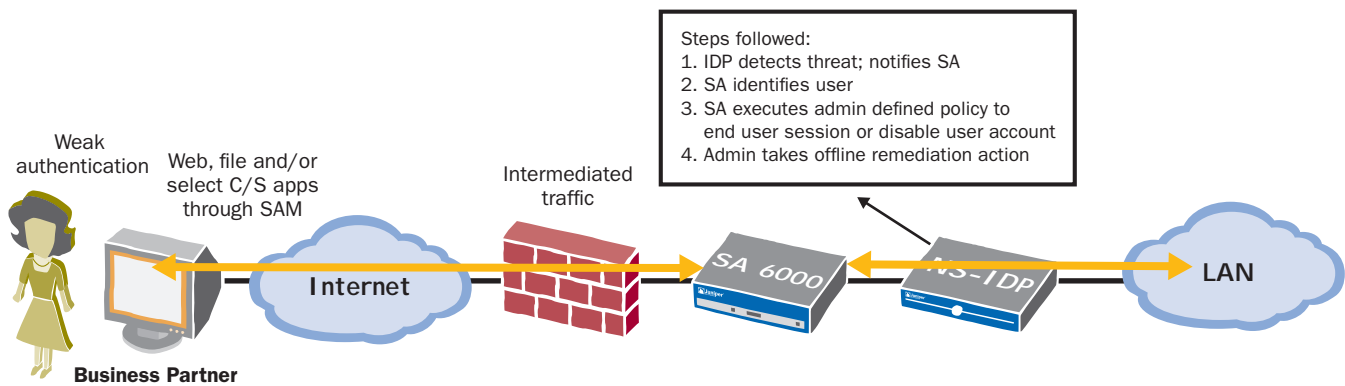


Diagram 3: Coordinated Threat Control for Partner Access



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

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
www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501