

Juniper Networks' unified access control solution leverages deep integration and interoperability between the Juniper Networks' NetScreen Firewall/VPN solutions and industry leading Content Management vendors to enable enterprises to deploy a best-in-class security solution that controls access, defeat threats, ensures compliance, and delivers secure and assured network services.

Content Management Alliances



Situation

Today's enterprises have evolved over the past decade to enable nearly ubiquitous connectivity for a host of different user groups, including remote/mobile employees, business partners, customers, onsite consultants, and more. Instant access has become almost expected regardless of the user location, be it as part of the extended enterprise, which can include home, hotels, or kiosks; the distributed enterprise, including branch offices; or the campus LAN. Resources and applications are presumed to be available whether they are located in the data center or on the Internet.

Unrestricted access has become commonplace, and so too have network security issues. Employee access to the Internet continues to introduce new dangers and content that can negatively impact your company in four fundamental ways:

Security Threats: Viruses, spyware and other malware can all enter your network through web-based e-mail, file downloads, Instant Messaging, P2P applications and other non-work related sites.

Legal Threats: Inappropriate content can lead to gender, minority or religious harassment and discrimination. Illegal downloading and distribution of copyrighted or illegal material over your network also has legal liability issues as well.

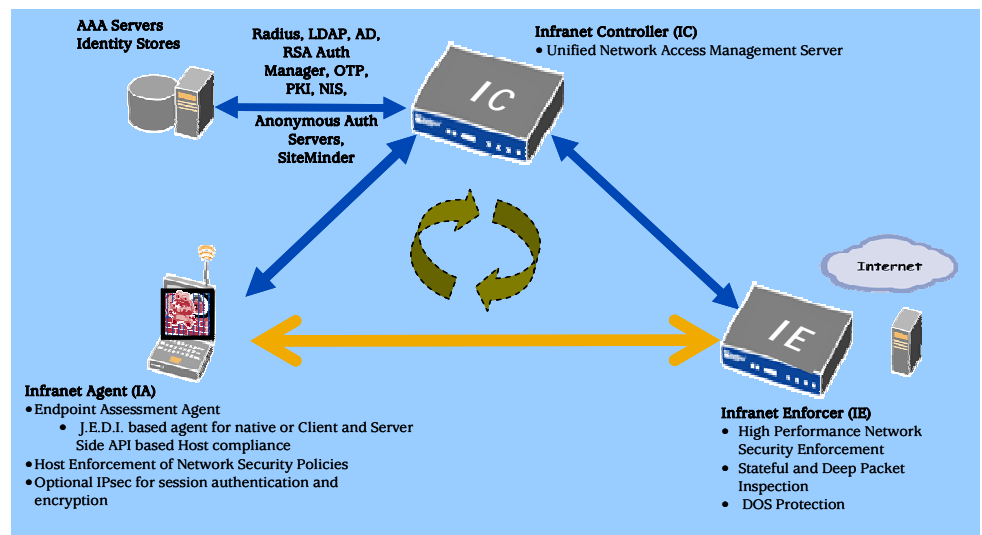
Productivity Threats: The temptations of non-work related Web destinations are endless. Just 20 minutes of recreational surfing a day can cost a company with 500 employees over \$8,000 per week. (estimated at \$50/hour/employee).

Network Threats: An employee can crash a network just by logging into the wrong website. Other activity like recreational surfing and downloading MP3 files can divert valuable bandwidth from critical business needs.

A critical challenge to network security has emerged, especially in the extended enterprise, with remote and mobile employees, business partners, customers and others accessing the enterprise network from unknown endpoints and untrusted networks.

Solution

Juniper Networks' unified access control solution has met this challenge, by creating a means to check an endpoint's security posture before access to the network and critical resources is allowed. The unified access control solution also leverages content management capabilities for access control, mapping users to specific areas of the network or to web content, based on roles and levels of trust established.



Content Management Alliances



The Juniper unified access control solution includes:

Infranet Controller: Leveraging Juniper's Secure Access SSL VPN policy and control engine to provide seamless communication with authentication servers, identity and authorization directory stores, the Controller enables session-specific, conditional access to networks based upon user authentication and a real-time check of the device's security characteristics.

Infranet Agent: Seamlessly provisioned by the Infranet Controller, the Infranet Agent is a lightweight software agent that assesses the endpoint's compliance state and communicates the resulting state back to the Infranet Controller. The Infranet Agent leverages diverse endpoint technologies and a rich range of endpoint security checks for comprehensive endpoint assessment. Based on the resulting state, the Infranet Agent can also enforce network policy on the client host, including both FW rules and dynamically provisioned IPSec VPN policy, if that is required.

In addition to client host enforcement, the first release of the Infranet Controller also supports enforcement on the entire line of Juniper firewall/VPN appliances and integrated security gateways.

Infranet Enforcers can support endpoint defense and provide end-to-end transport security, if required, by consuming signals from the Infranet Controller. The Infranet Enforcers achieve this increased policy control, as well as enhanced visibility into and protection of network transactions, without requiring significant infrastructure changes.

In essence, content management capabilities on the Infranet Enforcers can be dynamically leveraged by the Infranet Controller to provide comprehensive access control management.

Key Benefits

The combination of the Infranet Controller, Agent, and enforcement points provides enterprises high-availability, high-performance and reliability to ensure real-time network policy management without performance compromise.

Together, these products create a unified access control solution that functions as a service layer over an existing infrastructure, and can be cost effectively deployed in simple phases at critical points in the network.

www.juniper.net



CORPORATE HEADQUARTERS
AND SERVICE 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
Technical Support: 408-745-9500

ASIA PACIFIC REGIONAL
SERVICE HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suites 2507-11, 25/F
Asia Pacific Finance Tower,
Citibank Plaza
Central, Hong Kong
Phone: +852-2332-3636
Fax: +852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SERVICE
HEADQUARTERS
Juniper Networks B.V.
Beech Avenue 3
1119 RA Schiphol Rijk
Amsterdam, The Netherlands
Phone: 31-20-712-5700
Fax: 31-20-712-5901

ADDITIONAL SERVICE
LOCATIONS
Herndon, VA, USA
Ogden, UT, USA
Westford, MA, USA
Beijing, China
Sydney, Australia

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. 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.