

# Juniper Networks Infranet Controllers

## Provide unified access control for all users throughout your network



With the advent of virtual private networks (VPNs), companies began to face the challenge of offering valuable business assets to remote and mobile users in the extended enterprise. Juniper Networks solved this problem with the award-winning Secure Access SSL VPN, which effectively binds remote user identity with endpoint assessment for dynamic access privilege management.

As access has become more ubiquitous, however, the balancing act between the need for access to resources and the ability to secure them has grown past the extended enterprise to other key network deployments including the remote office/distributed enterprise, the server front end, WAN access, and the campus network. Enterprise users, business partners or guests with unmanaged or ill managed devices may become unknowingly infected when surfing the Internet or working remotely, then bring those infected devices directly into the network. Users accessing the WAN from within the LAN without any access controls can open the enterprise to a host of threats. Meanwhile the contents of vulnerable servers or those in the data center are becoming simultaneously more accessible and more mission-critical. Those accessing these servers from an inadequately protected endpoint can pose a risk and defeat regulatory compliance.

Enterprises need a solution that ties together all aspects of the user's identity, device, and network, and can uniformly enforce policy throughout these diverse groups, many of which they do not control.

### An Evolution and a Revolution

Juniper Networks solves the problem of access control with the Infranet Controller, available in two different form factors. These purpose-built, hardened appliances leverage Juniper's market-leading Secure Access SSL VPN policy control engine, which seamlessly integrates with the enterprise's existing AAA/identity and access management infrastructure. The appliance itself supports multi unit clustering and failover capabilities for optimal scalability and reliability, with operational convenience. Endpoint security state is assessed using the Infranet Agent, a lightweight agent that is dynamically downloaded from the Controller when a user first logs in. The results of this host assessment are combined with user identity and network information to create dynamic policies, which are then propagated throughout the network to enforcement points. These assessments can be repeated at administrator defined times during the session to ensure dynamic policy management and enforcement and also provide granular, policy-specific remediation capabilities for non-compliant users.

Phase One network-based enforcers include Juniper's market-leading NetScreen firewalls, which integrate policy findings using the latest version of ScreenOS code. Additional client-side enforcement is provided by the Host Enforcer Module, included as part of the Infranet Agent. This enables host based policy enforcement in network segments that do not include a supported network enforcement point.

Juniper's unified access control solution enables true LAN security, with minimal changes to network infrastructure. In fact, for companies that are already protected with Juniper's market-leading NetScreen firewalls, all that is required is the installation of the Infranet Controller. The Infranet Agent is dynamically downloaded to endpoints so there is no client-side software to install, configure, or maintain. The Infranet Controller can be set up in audit mode, to achieve visibility without enforcement. Enforcement points can also be set up in Transparent mode, which requires no rework of routing/policies or changes to the network infrastructure. Unified access control dynamically enforces policies on LAN for all network users whether the endpoint is managed or not.

### The Infranet Controller 6000

The Infranet Controller 6000 is designed for large enterprises, with the capabilities to handle tens of thousands of concurrent endpoints. The IC 6000 has a number of high availability features, including a hot swappable power supply that can be field upgraded, as well as a field-upgradeable hard disk. The IC 6000 can be deployed in multi unit clusters, to increase performance and provide additional scalability.

### The Infranet Controller 4000

The Infranet Controller 4000 is designed for the needs of medium enterprises or remote/branch offices. The IC 4000 will scale to handle thousands of concurrent endpoints, and can be deployed in cluster pairs for high availability.

### Value Summary

#### Unify Endpoint, Identity and Network Information for Real-time Policy Management

- Infranet Controller
  - Leverages the market-leading Juniper Secure Access SSL VPN policy control engine, field proven in thousands of deployments
  - Deep integration with AAA servers, RADIUS, LDAP etc
  - Purpose built hardened appliance comes in two form factors for highest security and reliability
  - Support for thousands of concurrent endpoints
  - Dynamically provisioned lightweight endpoint agent
  - Host Check for endpoint assessment
    - Native Functionality
    - APIs for leveraging third party endpoint solutions
  - Host Enforcer for dynamic host based enforcement of client side security policy
  - Windows Single SignOn integration
  - Optional, dynamically provisioned set up of authenticated and encrypted transport for session integrity and privacy
  - Granular remediation and quarantining capabilities

### Leverage Existing Security Investments

- No need to qualify new security solution
- Leverage existing AAA infrastructure
- Trusted Enforcement Points
  - Leverage NetScreen's best-in-class firewall VPNs, from the 5 Series to the 5000 Series and ISG platforms

- Infranet Agent

- Leverage architecture for integration with best-in-class third party security applications with Juniper's Endpoint Defense Initiative

### Unify Endpoint, Identity and Network Information for Real-time Policy Management

The Infranet Controller provides a unique ability to dynamically manage policy that ties user identity, network information and endpoint assessment with policy, and to propagate this information real-time throughout the network. This protection enables the enterprise to enforce policy across the network, regardless of whether the endpoint is owned by the enterprise or not.

Features	Benefits
<b>Infranet Controllers</b>	
Ability to bind endpoint assessment and user identity with real-time network security policy enforcement	<ul style="list-style-type: none"> <li>• Dynamically bind endpoint and user identity to set firewall configurations/rules in real-time</li> <li>• Enable dynamic activation of select enforcer capabilities, including Deep Inspection, antivirus, logging and URL filtering</li> </ul>
Leverages Juniper's Secure Access SSL VPN policy engine	The Secure Access appliance leads the market for SSL VPNs, and has been field-tested in thousands of deployments around the world
Two purpose-built, hardened form factors	<p>Allows the enterprise to choose the best fit for their needs:</p> <p><b>IC 6000</b></p> <ul style="list-style-type: none"> <li>• Supports up to 25,000 concurrent endpoints</li> <li>• Unique hardware features, including hot swappable power supply, hot swappable fan, field upgradeable hard disks</li> <li>• May be provisioned in multi-unit clusters</li> </ul> <p><b>IC 4000</b></p> <ul style="list-style-type: none"> <li>• Supports up to 3,000 concurrent endpoints</li> <li>• May be provisioned in cluster pairs</li> </ul>
Single centralized policy engine to enforce access controls before session login and throughout the session	<ul style="list-style-type: none"> <li>• User security state evaluated before users allowed to authenticate and throughout the session</li> <li>• Pre-authentication assessment, authentication, role mapping and resource controls all in one location</li> <li>• Easy setup and administration of network resource policy rules</li> <li>• No forklift upgrade of existing infrastructure is required to deploy the solution</li> <li>• Dynamic propagation of policy enforcement to enforcement points and to the endpoint</li> <li>• Policy can change as the endpoint or network environment changes</li> </ul>
Dynamic authentication policy leverages existing investment in AAA, including: <ul style="list-style-type: none"> <li>• RADIUS</li> <li>• LDAP</li> <li>• AD</li> <li>• RSA ACE</li> <li>• NIS</li> <li>• Certificate servers (digital certs/PKI)</li> <li>• Local login/password</li> <li>• Netegrity SiteMinder (Computer Associates)</li> <li>• RSA Cleartrust</li> <li>• Oblix (Oracle)</li> </ul>	Leverages the enterprise's existing investment in directories, PKI, and strong authentication, enabling administrators to establish a dynamic authentication policy for each user session
Dynamic role mapping	Leverages a range of attributes for security requirements that users need to meet before a user login page is presented. These security requirements can be enforced pre-authentication as well as post-authentication throughout the session.
Hybrid role- / resource-based policy model	<ul style="list-style-type: none"> <li>• User may be mapped to multiple roles</li> <li>• Administrators can tailor access to dynamically ensure that security policies reflect changing business requirements</li> </ul>
Granular auditing and logging	Ensures detailed logging by roles that end users belong to, resources that they are trying to access, and the state of compliance of the endpoint and user to the security policies of the network.
Custom instructions for granular quarantine and remediation of non-compliant users	<ul style="list-style-type: none"> <li>• Enables a self-administering platform that can intelligently quarantine non-compliant users and allow them to remediate without any assistance</li> <li>• Instructions can be specific to each security policy</li> <li>• Users are dynamically mapped to an access role upon remediation</li> </ul>
Windows Single SignOn (Advanced license)	Provided as part of the Infranet agent, Windows Single SignOn enables a seamless end user login experience in Active Directory environments.
Advanced role definition and mapping rules with custom expressions (Advanced License)	Custom rules using Boolean expressions allow still more flexibility in mapping users to roles and resources, by enabling the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level.

Features	Benefits
<b>Infranet Agent</b>	
Lightweight agent, dynamically provisioned by the Infranet Controller, if required. Includes: <ul style="list-style-type: none"> <li>• Host Checker (J.E.D.I)</li> <li>• Host Enforcer</li> <li>• MS Windows Single SignOn</li> <li>• Agentless enforcement for Mac and Linux</li> </ul>	<ul style="list-style-type: none"> <li>• IT departments are not required to deploy, install, configure or maintain software on corporate devices.</li> <li>• The enterprise can maintain access control, even if they do not own or manage the endpoint.</li> <li>• Protects authenticated endpoints from malicious/non-compliant endpoints</li> </ul>
Endpoint assessment, which can run at login and periodically throughout the user session at administrator-defined intervals	<p>Allows real-time network policy management. Provisioned with two different types of endpoint assessment, which can be combined:</p> <p><b>Host Checker</b> Native functionality:</p> <ul style="list-style-type: none"> <li>• Checks port activity, processes and registries, as well as performs an MD5 checksum to verify authenticity</li> <li>• Can be administrator configured to check: <ul style="list-style-type: none"> <li>– Source IP</li> <li>– AV vendor and host intrusion prevention software</li> <li>– Personal firewall, anti-spyware, and malware solutions</li> <li>– OS version</li> <li>– Hot fix/patch management</li> </ul> </li> </ul> <p><b>Juniper Endpoint Defense Initiative (J.E.D.I)</b></p> <ul style="list-style-type: none"> <li>• Leverage existing best-in-class third party security applications via the J.E.D.I. open API framework</li> <li>• Client-side APIs check to ensure that the required application is running</li> <li>• Server-side APIs enable the application to be downloaded if it is not on the device</li> </ul>
Host Enforcer <ul style="list-style-type: none"> <li>• Client Firewall Policy Enforcer</li> <li>• Optional secure transport (authenticated and encrypted) using IPSec</li> </ul>	<ul style="list-style-type: none"> <li>• Provides firewall policy if endpoint is accessing a network segment not protected by an Infranet Enforcer</li> <li>• Optional Microsoft IPSec enforcement provides authenticated and encrypted transport for session integrity and privacy</li> <li>• Gives administrators an easy way to provision authenticated and encrypted transport for session integrity and privacy <ul style="list-style-type: none"> <li>– Authenticated transport ensures that network rules can be enforced in a secure manner</li> <li>– Encrypted transport ensures privacy for communications on the LAN</li> </ul> </li> </ul>
Agentless deployment for cross platform support	Enterprises can secure Mac and Linux endpoints by binding endpoint assessment and user identification for source IP-based enforcement of network security policies

### Leverage Existing Security Investments

Juniper's unified access control solution enables the enterprise to make the most out of their security investments. The Infranet Controller leverages the existing AAA infrastructure and uses existing Juniper firewall/VPN platforms as enforcement points for policy.

The Infranet Agent also leverages existing security applications with Host Checker's open APIs and Juniper Endpoint Defense Initiative (J.E.D.I) alliances. This enables easy provisioning of these applications, in addition to native host checking capabilities.

Features	Benefits
<b>Infranet Enforcers – Phase One</b>	
Leverage Juniper's market-leading range of firewalls, including: <ul style="list-style-type: none"> <li>• Juniper Networks NetScreen-HSC</li> <li>• Juniper Networks NetScreen-5 Series</li> <li>• Juniper Networks NetScreen-25</li> <li>• Juniper Networks NetScreen-50</li> <li>• Juniper Networks NetScreen-200 Series</li> <li>• Juniper Networks NetScreen-500 Series</li> <li>• Juniper Networks NetScreen-5000 Series</li> <li>• Juniper Networks ISG Series</li> </ul>	The Infranet Controller dynamically provisions access policy to Juniper firewalls, enabling "one-box access control" for existing Juniper-protected networks.
Juniper's range of firewalls provide industry-leading packet performance, with throughput from 75 Mbps to 30 Gbps	Juniper has a firewall that is optimized for all enterprise deployments, from SME users to the largest enterprise.
Integrates stateful and deep packet inspection, Anti-X technology, and DoS/DDoS protection	Juniper's best-of-breed Firewall/VPN solutions protect enterprises of all sizes by integrating in-depth protection against blended and traditional network attacks.
Ability to bind endpoint assessment and user identity to set firewall configurations/rules in real time	Enables Juniper's firewalls to react to changing network conditions, and not just static rules
<b>Open Standards-based APIs</b>	
Open standards-based J.E.D.I APIs enable endpoint assessment integration with best-in-class third party vendors	Enables enterprises to easily leverage their existing investment in third party security applications.

## Specifications

### Upgrade Options

#### Hardware – IC 6000 Only

- Redundant hot-swappable hard disk (upgrade option)
- Redundant hot swappable power supply (upgrade option)

#### Software – IC 4000 and IC 6000

- Advanced Software Feature Set (includes Central Manager)

## Technical Specifications

### IC 4000

- Dimensions: 16.7”W x 1.74”H x 15”D (42.42cmW x 4.41cmH x 38.10cmD)
- Weight: 13.6lb (6.17kg) typical (unboxed)
- Material: 18 gauge (.048”) cold-rolled steel
- Fans: 3 40mm ball bearing fans, 1 40mm ball bearing fan in power supply

### IC 6000

- Dimensions: 16.7”W x 3.5”H x 16.2”D (42.42cmW x 8.89cmH x 41.15cmD)
- Weight: 28.5lb (12.94 kg) typical (unboxed)
- Material: 18 gauge (.048”) cold-rolled steel
- Fans: 2 externally accessible, hot swappable ball-bearing fans

### Panel Display – IC 4000

- Front Panel Power Button
- Power LED, HD Activity, Temp

### Panel Display – IC 6000

- Front Panel Power Button
- Power LED, HD Activity, Temp, PS Fail
- HDD Activity and RAID Status LEDs

### Console – IC 4000 and IC 6000

- One 9-pin serial console port

### Ports – IC 4000 and IC 6000

- Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)

### Power – IC 4000

- AC Power Wattage 260 Watts
- AC Power Voltage 100-240VAC, 50-60Hz, 2.5A Max
- System Battery CR2032 3V lithium coin cell
- Efficiency 65 % minimum, at full load
- MTBF – 82khrs

### Power – IC 6000

- AC Power Wattage 500 Watts
- AC Power Voltage 100-240VAC, 50-60Hz, 5A Max
- System Battery CR2032 3V lithium coin cell
- Efficiency 65 % minimum, at full load
- MTBF – 71khrs

### Environmental

- Operating Temp 50° to 95°F (10°C to 35°C)
- Storage Temp -40° to 158°F (-40°C to 70°C)
- Relative Humidity (Operating) 8% to 90% noncondensing
- Relative Humidity (Storage) 5% to 90% noncondensing
- Altitude (Operating) -50 to 10,000 ft (3,000m)
- Altitude (Storage) -50 to 35,000 ft (10,600m)

### Safety and Emissions Certification

- Safety: EN60950-1:2001 + A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
- Emissions: FCC Class A, VCCI Class A, CE class A

### Warranty

- 90 days – can be extended with support contract



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

## Ordering Information

### Infranet Controller 4000

#### Base System

IC4000 Enterprise Infranet Controller 4000 Base System

#### Endpoint Licenses

IC4000-ADD-100E	Add 100 simultaneous users to IC4000
IC4000-ADD-250E	Add 250 simultaneous users to IC4000
IC4000-ADD-500E	Add 500 simultaneous users to IC4000
IC4000-ADD-1000E	Add 1000 simultaneous users to IC4000
IC4000-ADD-2000E	Add 2000 simultaneous users to IC4000
IC4000-ADD-3000E	Add 3000 simultaneous users to IC4000

#### Feature Licenses

IC4000-ADV Advanced for IC4000

#### Clustering Licenses

IC4000-CL-100E	Clustering: Allow 100 additional users to be shared from another IC4000
IC4000-CL-250E	Clustering: Allow 250 additional users to be shared from another IC4000
IC4000-CL-500E	Clustering: Allow 500 additional users to be shared from another IC4000
IC4000-CL-1000E	Clustering: Allow 1000 additional users to be shared from another IC4000
IC4000-CL-2000E	Clustering: Allow 2000 additional users to be shared from another IC4000
IC4000-CL-3000E	Clustering: Allow 3000 additional users to be shared from another IC4000

### Infranet Controller 6000

#### Base System

IC6000 Enterprise Infranet Controller 6000 Base System

#### Endpoint Licenses

IC6000-ADD-250E	Add 250 simultaneous users to IC6000
IC6000-ADD-500E	Add 500 simultaneous users to IC6000
IC6000-ADD-1000E	Add 1000 simultaneous users to IC6000
IC6000-ADD-2000E	Add 2000 simultaneous users to IC6000
IC6000-ADD-3000E	Add 3000 simultaneous users to IC6000
IC6000-ADD-5000E	Add 5000 simultaneous users to IC6000
IC6000-ADD-10000E	Add 10000 simultaneous users to IC6000
IC6000-ADD-15000E	Add 15000 simultaneous users to IC6000
IC6000-ADD-20000E	Add 20000 simultaneous users to IC6000
IC6000-ADD-25000E	Add 25000 simultaneous users to IC6000

#### Feature Licenses

IC6000-ADV Advanced for IC6000

#### Clustering Licenses

IC6000-CL-250E	Clustering: Allow 250 additional users to be shared from another IC6000
IC6000-CL-500E	Clustering: Allow 500 additional users to be shared from another IC6000
IC6000-CL-1000E	Clustering: Allow 1000 additional users to be shared from another IC6000
IC6000-CL-2000E	Clustering: Allow 2000 additional users to be shared from another IC6000
IC6000-CL-3000E	Clustering: Allow 3000 additional users to be shared from another IC6000
IC6000-CL-5000E	Clustering: Allow 5000 additional users to be shared from another IC6000
IC6000-CL-10000E	Clustering: Allow 10000 additional users to be shared from another IC6000
IC6000-CL-15000E	Clustering: Allow 15000 additional users to be shared from another IC6000
IC6000-CL-20000E	Clustering: Allow 20000 additional users to be shared from another IC6000
IC6000-CL-25000E	Clustering: Allow 25000 additional users to be shared from another IC6000

#### Accessories

IC6000-HD	Field Upgradeable Secondary Hard Disk for IC6000
IC6000-FAN	Field Upgradeable Fan for IC6000
IC6000-PS	Field Upgradeable Secondary Power Supply for IC6000
SA-ACC-RCKMT-KIT-1U	Secure Access and Infranet Controller Rack Mount Kit - 1U
SA-ACC-RCKMT-KIT-2U	Secure Access and Infranet Controller Rack Mount Kit - 2U
SA-ACC-PWR-AC-UK	Secure Access and Infranet Controller AC Power Cord UK
SA-ACC-PWR-AC-EUR	Secure Access and Infranet Controller AC Power Cord EUR
SA-ACC-PWR-AC-JPN	Secure Access and Infranet Controller AC Power Cord JPN

Copyright 2005, Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.