

INSTANT VIRTUAL SYSTEM FOR SA SERIES SSL VPN APPLIANCES

Product Overview

Juniper Networks IVS solution is the industry's first end-to-end SSL VPN virtualization framework designed to enable administrators to provision 240 logically independent SSL VPN gateways within a single appliance/cluster. This enables Service Providers (SPs) to offer network-based SSL VPN managed services to multiple customers from a single device or cluster, as well as enabling enterprises to completely segment SSL VPN traffic between multiple groups. IVS features complete application-layer, network-layer and access management virtualization, so that end customers of SPs or groups within enterprises can have the experience of their own SSL VPN deployment, while the SP or enterprise administrator only has to manage one device or cluster. IVS software can be provisioned on a variety of Juniper Networks SSL VPN platforms, both by SPs and by enterprises.

Product Description

Juniper Networks[®] Instant Virtual System (IVS) enables complete customer separation and provides segregation of traffic between multiple customers using granular role-based VLAN (802.1Q) tagging. This enables the secure segregation of end users' traffic, even if two customers have overlapping IP addresses, and enables provisioning of specific VLANs for different user constituencies, such as remote employees and partners of customers. Domain Name System (DNS)/Windows Internet Name Service (WINS), Authentication, Authorization and Accounting (AAA), log/accounting servers and application servers such as Web mail, file shares, etc. can reside either in the respective customers' intranets or in the SP network. SPs can provision an overall concurrent number of users on a per customer basis with the flexibility to distribute further amongst different user audiences such as remote employees, contractors, partners, etc.

Like all products built on the Instant Virtual Extranet (IVE) platform, IVS is based on the use of SSL available in all Web browsers as a means of secure transport. This enables the SP to offer customers a means of remote access for their mobile employees and contractors without deploying any client software on devices, as well secure extranet or intranet access with no DMZ buildout, server hardening, Web agent deployments, or ongoing maintenance.

Architecture and Key Components

SPs can provision IVS to cost-effectively offer high return differentiated services such as remote employee and extranet access, business continuity, intranet LAN security and mobile device access to many customers from a single platform or cluster. End customers can be assigned a single virtual system with the flexibility to create multiple hostnames/sign-in URLs for user subgroups. SPs also have the flexibility of offering different VLANs for each subgroup of an enterprise, should intra-group traffic need to be segmented. This feature can aid in regulatory compliance and raise security, without adding any additional equipment for the end customer to manage. SPs can tailor their offerings, and they can control the degree of customer management and configuration that they wish to offer to their end customers. For example, an SP can choose whether they wish to delegate the ability for end customers to establish their own customized user portal, endpoint security, authentication, authorization and auditing policies or whether they would prefer to limit the offering to predefined standards.

Instant Virtual Systems for the Enterprise

The IVS solution can also be used within enterprises, should an organization want to deploy a highly available SSL VPN solution with granular, group-based VLANs in order to provide traffic segregation between multiple groups/domains. One such deployment could be in the case of a corporate headquarters, where the enterprise wanted to provide connectivity to branch offices. IVS could be used to create a virtual system for each branch office, allowing administrators in those offices to manage their own SSL VPN virtual system, while not being able to view or modify information on another branch's virtual system. This use case offers a high degree of flexibility while allowing corporate headquarters to retain ultimate control of the system and ensure regulatory compliance.

Features and Benefits

Multiple Virtual Systems from One Platform/Cluster

IVS enables administrators to provision customer/group specific virtual systems each with unique virtualization definitions for network, security (endpoint, authentication, authorization and auditing), and management policies.

FEATURE	BENEFITS
Virtualized Network Settings	
<ul style="list-style-type: none">• Highly granular role based VLAN (802.1Q) tagging support for Core, Secure Application Manager (SAM) and Network Connect (NC) access methods• Up to 240 VLANs, each with its own route table and with VLAN IDs configurable in the range of 1 to 4095, can be provisioned on the fly, without requiring a system reset• Virtualized DNS/WINS Settings• Overlapping IP addresses support across Instant Virtual Systems	<ul style="list-style-type: none">• Enables administrators to define one or more unique 802.1Q VLAN tags on a role basis within each customer/group specific virtual system• Enables SPs/enterprises to maintain complete logical separation between multiple customers/groups when shared on a single appliance/cluster• With a configurable VLAN ID range and dynamic addition & deletion of VLANs, new customers/groups can be provisioned without interrupting existing customers' traffic• Ability to configure overlapping IP addresses for application and authentication servers across intranets of multiple customers shared on the same appliance/cluster• Administrators can also provision static IP address pools with overlapping IP addresses for NC end users across multiple customers
Virtualized System Settings	
<ul style="list-style-type: none">• Fully customizable look and feel at the end user level with one or more sign-in URLs (hostnames)• Flexibility in defining per customer authentication and authorization servers• Controlled, distributable concurrent user counts	<ul style="list-style-type: none">• Administrators can assign one or more sign-in URLs per customer/group and offer complete flexibility to customize the UI for unique look and feel• Ability to create a standard portal look and feel for quick rollout• Ability to configure one or more authentication servers per customer with the flexibility to select different server types for authorization• Seamless integration with existing directory infrastructure in customers' networks• Ability to provision an overall concurrent number of users on a per customer/group basis with the flexibility to distribute it further amongst different user audiences such as remote employees, contractors, partners, etc.
Configurable Security and Access Policies	
<ul style="list-style-type: none">• Authentication & authorization policies to control end user access privileges• Endpoint security policies to assess device/network security state• Comprehensive application layer and network layer access methods with granular access controls• Auditing and logging	<ul style="list-style-type: none">• SPs can standardize offerings or offer differentiated services with flexibility to create security policies on a per customer basis that meet specific end user access privilege requirements• Granular access privileges for variety of end user constituencies such as employees, contractors, partners, etc.• Multiple customers on a shared single system can have entirely different or overlapping endpoint security policies• Can standardize offerings, or create differentiated services with the flexibility to create customer specific policies that reflect their own end user base needs• Each access method provides different levels of access control, from IP addresses, all the way to the URL or file level• SPs can offer auditing and logging services or end customers can use their own log/accounting servers• With log data, SPs can help end customers with regulatory compliance

Streamlined Administration with Role-Based Delegation

IVS provides streamlined administration to most efficiently provision multiple customers/groups. It also features standards-based management protocols to facilitate integration with third-party management and reporting products.

FEATURE	BENEFITS
Advanced role based delegation and management policies for: <ul style="list-style-type: none"> • Customer administrators within an IVS • SP administrators across IVSs 	<ul style="list-style-type: none"> • Flexibility to delegate customer portal administration, customer specific logs and usage monitoring, end user access privileges and endpoint security policies • Delegated administrator roles requiring single or dual factor authentication can be created for customer administrators within an IVS or for internal SP administrators across IVSs with the ability to: <ul style="list-style-type: none"> – Provision read/write, read only access – Granularly delegate out individual tasks with read/write/deny privileges for each task
Syslog and usage monitoring	<ul style="list-style-type: none"> • Virtualization of logs enables dynamic filtering of user and administrator access logs for each customer • With log data, SPs can help end customers with regulatory compliance • Ability to restrict a customer administrator to only view and/or export logs specific to that customer • Syslog data can be generated on a per customer basis even when multiple customers are hosted on the same system • Multiple syslog servers per customer allows syslog data to be sent to servers in the customer network and/or in the SP for record keeping and duplication purposes
RADIUS accounting	<ul style="list-style-type: none"> • Customer specific RADIUS accounting facilitates seamless billing integration with existing billing applications • Flexibility to enable RADIUS accounting even when authentication server type is different than RADIUS
SNMP	<ul style="list-style-type: none"> • Customer specific maintenance and troubleshooting with virtualized SNMP traps for major and critical events • Real time system health monitoring with SNMP MIBs for critical parameters such as CPU and memory utilization, concurrent number of users
Troubleshooting and diagnostics	<ul style="list-style-type: none"> • Virtualized troubleshooting and diagnostics enable SPs to service individual customers without affecting other customers hosted on the same system
IVS Shared Authentication Services	<ul style="list-style-type: none"> • Allows IVS customers to provide access to authentication services that can be shared across virtual systems • Allows the customer to place the authentication service on a particular VLAN and share that VLAN across all IVS on a given system or cluster

Virtualized Best-in-Class SSL VPN Features that End Users Demand

Juniper Networks market leading SSL VPN offerings provide an unmatched feature set. These features are available to end customers as part of a virtualized system, allowing the SP to choose to offer them as part of a standard or differentiated service offering. More detailed information on the standard Juniper Networks SSL VPN features can be found in the SA Series SSL VPN Appliances datasheet.

CLASSIFICATION	SPECIFIC FEATURES
Access privilege management capabilities	<ul style="list-style-type: none"> • Hybrid role- and resource-based policy model • Pre-authentication assessment • Dynamic authentication policy • Dynamic role mapping • Resource authorization • Granular auditing and logging • Extensive directory integration & broad interoperability
Provision by purpose	<ul style="list-style-type: none"> • Clientless Core Web access—Access to Web-based applications, including complex JavaScript, XML or Flash-based apps and Java applets that require a socket connection, as well as standards-based email like Outlook Web Access (OWA), Windows and UNIX file share, telnet/SSH hosted applications, Terminal Emulation, Sharepoint, and others. • Secure Application Manager (SAM)—A lightweight Java or Windows-based download enables access to client/server applications using just a Web browser. Also provides native access to terminal server applications without the need for a pre-installed client. • Network Connect—Provides complete network-layer connectivity via an automatically provisioned, cross platform download from a Web browser. Adaptive dual mode transport for optimal network layer connectivity in diverse connection environments.

Virtualized Best-in-Class SSL VPN Features that End Users Demand (continued)

CLASSIFICATION	SPECIFIC FEATURES
End-to-end layered security	<ul style="list-style-type: none">• Host Checker• Host Checker API• Trusted Network Connect (TNC) Support on Host Checker• Policy-based enforcement and remediation• Hardened Security Appliance• Secure Virtual Workspace• Cache Cleaner• Integrated Malware Protection
User self-service features	<ul style="list-style-type: none">• Password management integration• Web-based Single Sign-On<ul style="list-style-type: none">– BASIC Auth & NT LAN Manager (NTLM), Forms-based, Header Variable-based, SAML-based

Performance-Enabling Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains, faster rollouts of new business models and ventures, and greater market reach, while generating higher levels of customer satisfaction. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/products-services.

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.

Ordering Information

MODEL NUMBER	MODEL NAME AND DESCRIPTION
SA4500-IVS	Instant Virtual Systems for SA4500
SA6500-IVS	Instant Virtual Systems for SA6500



Tel North: 0151 2031400 Tel South: 0118 9071600
Email: info@castleforce.com Web: 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. "Engineered for the network ahead" and JUNOSe are trademarks 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.

