

## What's New in Juniper's IVE Platform Version 5.1

This application note describes the new features available in Version 5.1 of the IVE platform for all Secure Access products. This document assumes familiarity with the Juniper's IVE platform and the features of earlier releases up to version 5.0.

### Highlights of this Release

Juniper Networks enables enterprises and service providers to converge all their secure access needs to provide secure and assured communication experience with the 5.1 version of the IVE platform:

#### **I. Introduction to Secure Access New Licensing Model**

#### **II. Core Clientless Access Support for the SA700**

#### **III. Increased Ease of Use and Deployment**

- **Advanced Certificate Infrastructure Enhancements**
  - **Online Certificate Status Protocol (OCSP) Support**
  - **CRL Partitioning Support**
  - **Dynamic Learning of Intermediate CAs**
- **Multiple File Upload/Download Support**
- **Sign IVE Java Applets and ActiveX Controls**

#### **IV. Introduction to the Instant Virtual System (IVS)**

- **Industry's first end to end virtualization framework**
  - **255 Virtual SSL VPN Gateways within a single appliance / cluster**
  - **Application Layer, Network Layer and Access Management Virtualization**
- **Customer / Group specific Virtual Systems**
- **Granular Role based VLAN (802.1Q) Tagging for Core, SAM and NC**
- **Overlapping IP Addresses support across Virtual Systems**

## **I. Introduction to Secure Access New Licensing Model**

With IVE v5.1, Juniper has introduced a new licensing model to meet customers' needs. Licenses will be maintained by a 24-7 online system (Licensing Management System or LMS) available on the Juniper website ([http://www.juniper.net/generate\\_license](http://www.juniper.net/generate_license)).

*User Licenses* enable you to support as many concurrent users as specified in the license for Juniper's Baseline features and for all the feature licenses you have bought and installed. User Licenses are additive. For example: if you purchase two 100 concurrent users licenses the Secure Access appliance will support 200 concurrent users.

*Feature Licenses* will enable specific features on your Secure Access appliance (e.g. Advanced or Secure Meeting) for the number of concurrent users enabled on the appliance (or the cluster).

*Clustering Licenses* enable clustering among Secure Access products. You should always satisfy the following premise: the clustering user license on each appliance in the cluster should equal the user license on the primary appliance. For example: if you purchase a 250 concurrent users license for the primary appliance you will need a 250 users clustering license for every other appliance in the cluster.

*Lab licenses* are designed to allow you to deploy new SSL VPN functionality in a "test", "lab", or "pilot" environment before deciding to roll it out to your production environment. Lab licenses are valid for 52 weeks and will support all SSL VPN features.

### **Customer Benefits**

- Improved customer service by enhanced licensing management and tracking through the LMS
- Simplified licensing model for easy user-count and feature upgrades

### **Availability**

- All Secure Access Products

## **II. Core Clientless Access Support for the SA700**

With IVE v5.1, new and existing SA700 (formerly known as the RA500) customers will be able to purchase a license enabling Juniper's market-leading Core Clientless Access functionality including: (1) Web rewriting; (2) File browsing; (3) Terminal sessions (e.g. Telnet and SSH); (4) Pass-through proxy; and (5) Email client.

### **Customer Benefits**

- Clientless access to web-based applications and files in small enterprise deployments

### **Availability**

- Secure Access 700 with Core License

### **III. Increased Ease of Use and Deployment**

#### **1. Advanced Certificate Infrastructure Enhancements**

With IVE v5.1, Juniper has extended its support for environments with complex PKI infrastructure by adding support for the following features:

##### **1.1 Online Certificate Status Protocol (OCSP) Support**

With this feature, Juniper Networks provides the ability to be deployed in environments where OCSP is used for certificate revocation checking. OCSP is useful in determining the current status of a digital certificate without requiring the management of Certificate Revocation Lists (RFC 2560). In lieu of or as a supplement to checking against a periodic CRL, OCSP allows customers to obtain timely information regarding the revocation status of a certificate.

##### **1.2. CRL Partitioning Support**

Enhancing its Certificate Revocation List (CRL) support, Juniper Networks has added the ability to check for certificate revocation when the CRL is partitioned. Partitioned CRLs are CRLs stored in multiple entries. The IVE can query the CRL Distribution Point (CDP) to get an appropriate CRL based on the client certificate.

##### **1.3. Dynamic Learning of Intermediate Certificate Authorities**

With IVE v5.1, Juniper enhanced its client certificate revocation check by dynamically learning and installing intermediate CAs. An intermediate CA is added automatically with the default configuration and the Administrator can further refine the configuration manually after the installation.

#### **Customer Benefits**

- Ability for administrators to support diverse PKI deployments with greater flexibility
- Enhanced security by real-time enforcement of policy changes

#### **Availability**

- Secure Access Products with Advanced License

#### **2. Multiple File Upload and Download.**

Juniper Networks now supports the upload and download of multiple files. While browsing files, a user can select multiple files or folders to download to their device. The files and/or folders are downloaded as a single zipped folder. Similarly, the user can upload multiple files by clicking on upload and browse to the locations of the files. As before, to upload a folder, the user must first zip the folder and then upload the resultant zipped file. In this version, the user now has the option to uncompress .zip files and thus can directly add folders on the target server from their remote device.

#### **Customer Benefits**

- Improves user file browsing experience

### **Availability**

- All Secure Access Products (SA700 with Clientless Core Access License)

### **3. Sign IVE Java Applets and ActiveX Controls.**

This feature will provide administrators the ability to sign the IVE's Java applets and ActiveX controls such that any pop-ups from applets/controls that appear during IVE session do not have to say Juniper Networks. Administrators can now present pop-ups that are signed by their own certificate further allowing them to customize the user experience.

### **Customer Benefits**

- Allows greater customization of overall user experience
- Potentially prevents help desk calls from users concerned about pop-ups from an unexpected source

### **Availability**

- All Secure Access products (SA700 with Clientless Core Access License)

## **IV. Introduction to the Instant Virtual System (IVS)**

### **1. Industry's first End to End Virtualization Framework**

Virtualization framework with Application Layer, Network Layer and Access Management virtualization enables administrators to provision 255 logical independent SSL VPN gateways within a single appliance / cluster. Each virtual SSL VPN gateway represents a customer of a Managed Service Provider or a group within an enterprise providing complete segregation of traffic belonging to those customers/groups.

### **Customer Benefits**

- Enables Service Providers to offer highly available and scalable Network Based (Shared) SSL VPN Managed services to multiple enterprises of any size from a single appliance / cluster in a cost effective manner
- Allows Service Providers to create new revenue opportunities and increase customer satisfaction by bundling managed extranet access services, mobile device access services, intranet LAN Security (securing WLAN and VoIP) services and disaster recovery services along with employee remote access services

### **Availability**

- Secure Access products (SA3000 and above) with Instant virtual System (IVS) license

### **1.1 Customer / Group Specific Virtual Systems in a single appliance / cluster**

This feature enables administrators to instantiate customer / group specific virtual systems each with its own virtualization definitions for:

- VLANs (802.1Q tagging)
- DNS/WINS

- One or more Sign-in URLs (Host Names) and Realms
- Roles and Resource policies (End user access privileges)
- Authentication Server
- Concurrent users
- Host checking Policies
- Syslog and Usage Monitoring
- SNMP Traps for Major and Critical events
- RADIUS Accounting
- Role based Delegated Admin
- Troubleshooting and Diagnostics

#### **Customer Benefits**

- Enables Service Providers to define advanced customer specific SLAs (Service Level Agreements) for multiple customers hosted on a single appliance / cluster and manage them in a streamlined fashion
- Customer specific RADIUS accounting facilitates seamless billing integration with existing billing application and other managed services offered by the Service Provider
- Advanced role based delegation / management policies within an IVS and across IVSes allow service providers to own the management of the equipment and at the same time provide them the flexibility to delegate customer portal administration, customer specific logs and usage monitoring, end user access privileges and host checking policies

#### **Availability**

- Secure Access products (SA3000 and above) with Instant virtual System (IVS) license

### **1.2 Granular Role based 802.1Q VLAN Tagging within an IVS for Core, SAM and NC**

This feature enables administrators to define one or more unique 802.1Q VLAN tags on a role basis within each customer / group specific virtual system. Up to 255 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 system reset) in a single appliance / cluster. VLAN tagging can be configured for all three access methods – Core, SAM (Secure Application Manager) and NC (Network Connect).

#### **Customer Benefits**

- Customer specific VLAN(s) assignment enables service providers to maintain complete separation between multiple customers
- Define distinguished SLAs for end users and partners of a managed services customer

- Configurable VLAN ID range and dynamic addition / deletion of VLANs enable services providers to seamlessly provision VLANs in an end to end fashion in their networks without interrupting existing customers traffic
- Enables enterprises to deploy group based VLANs with granular access privileges and provide traffic segregation between multiple groups

#### **Availability**

- Secure Access products (SA3000 and above) with Instant virtual System (IVS) license

### **1.3. Overlapping IP addresses support across virtual systems**

This feature enables configuring overlapping IP addresses for application and authentication servers across intranets of multiple customers shared on the same appliance / cluster. Administrators could also provision static IP address pools with overlapping IP addresses across NC end users of multiple customers using this feature.

#### **Customer Benefits**

- Allows flexibility in hosting multiple customers with same intranet IP addresses as well as end users IP addresses on the same appliance / cluster

#### **Availability**

- Secure Access products (SA3000 and above) with Instant virtual System (IVS) license