COSINE INGAGE™

Customer Network Management System

- **Per-Customer Architecture**
- **Complete VPN Visibility**
- **Unprecedented Control**
- **Detailed Reports**

Visibility and Control for Enterprise Customers

The InGage Customer Network Management (CNM) solution is the industry's first per-customer reporting and control system optimized specifically for network-based service delivery. Efficient and scalable, InGage CNM arms you and your enterprise customers with unprecedented visibility and control across virtually every aspect of each customer's suite of network-based managed IP services, including firewall services, remote access services and a multitude of Virtual Private Network (VPN) services.

InGage works in conjunction with the IPSX™ IP Service Switches and InVision™ Services Management System (SMS) to provide an inherently efficient mechanism for reporting on each customer's unique suite of managed IP services.

Unlike other systems, InGage CNM does not require an expensive and operationally complex overlay of software agents and hardware probes collecting data from Customer Premises Equipment (CPE) and desktops installed at thousands of customer sites. Nor does it require a complex web of collector servers and aggregator servers to capture and massage data into per-customer views.

Unique Per-Customer Architecture

The InGage CNM leverages CoSine's inherent per-customer architecture—collecting per-customer metrics and configuration information from your existing IPSX switches and InVision SMS.

The per-customer services virtualization architecture also means that visibility into the full range of services that make up each customer's managed IP services—typically a diverse mix of different types of VPNs, firewalls, Network Address Translation (NAT) and remote access services—are now at their fingertips. InGage CNM efficiently collects detailed per-site and per-service usage, performance, Service Level Agreements (SLAs), firewall activity, policy and configuration data and formats these into per-customer reports in Adobe Acrobat format, as well as easily exported XML structured data. Internal staff, who are responsible for assisting customers, are now empowered to better enforce enterprise-wide policies, measure performance against SLAs, speed problem resolution, leverage trend analysis, dramatically improve planning and communicate critical information to senior management.

Vast Reporting Capability

With InGage CNM, you can efficiently produce straightforward and detailed reports on virtually every aspect of each customer's managed IP services portfolio. Advanced reporting capabilities allow you to:

- Attract more conservative customers to managed IP services by removing visibility as a barrier to entry for customers considering transitioning from managed Frame Relay services or from private security solutions.
- Further differentiate managed IP services from competitors' offerings and from private solutions by offering efficiently delivered rich reporting.
- Relieve the considerable burden of enterprises having to build and rationalize a multitude of private reporting systems and providing reporting to customers who could never afford to build it on their own.
- Improve customer satisfaction by augmenting your help desk, Network Operation Center (NOC) and engineering operations with a level of granular per-customer information not available from other solutions.

Detailed Data Access Enables Service Enhancements

By producing such a rich breadth of data in an efficient, carrier-scaled delivery model, InGage CNM solves several problems. You can now:

- Add tiers to the managed IP services portfolio by offering a range of basic and premium services (e.g., Bronze, Silver, Gold) whose pricing depends on the richness and frequency of reporting.
- Innovate on pricing plans by leveraging InGage's rich per-customer usage data collection. For example, you could create a burstable VPN service based on 95th percentile usage mapped against pricing tiers, a firewall service priced according to session usage or a VPN-wide pricing scheme pegged to aggregate usage across all the customer's sites.
- Enrich business intelligence/data mining initiatives for more tailored product development and customer outreach by exporting InGage's per-customer XML structured data into your business intelligence systems.
- Strengthen the bond of trust with customers of outsourced services.
- Reinforce brand awareness with customers by using your logos or illustrations on InGage-generated reports and by customizing views and templates for different market segments.
- Engage in a more strategic relationship with the customer. For example, you can leverage the availability of rich customer-specific data for joint analysis and planning with the customer.

With these powerful InGage CNM capabilities, you can attract new customers, up-sell managed IP services, boost loyalty and reduce churn.

FASST™
FLEXIBLE ARCHITECTURE FOR SUBSCRIBER SERVICE TERMINATION

CoSine® COMMUNICATIONS

FUJITSU
THE POSSIBILITIES ARE INFINITE

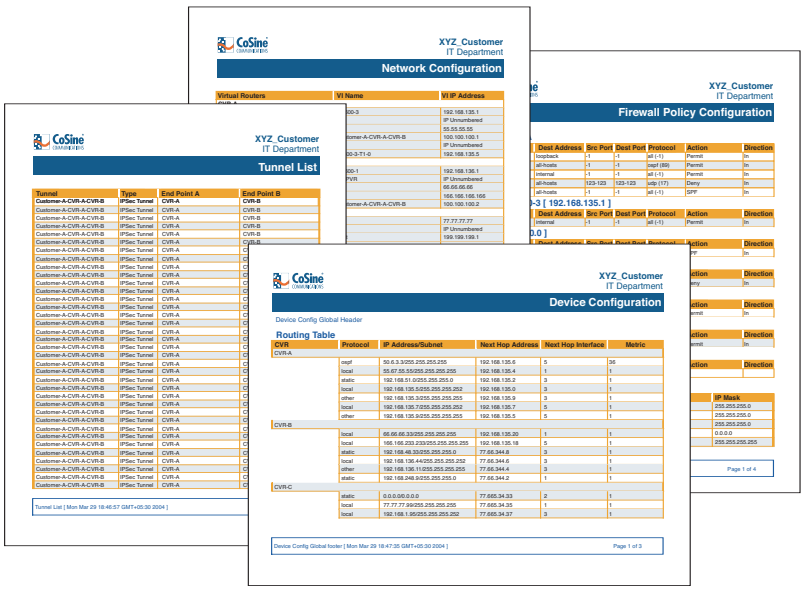
COSINE INGAGE™

Policy and Configuration Reporting

Through InGage's policy and configuration reports, all of the customer's Virtual Routers (VRs), as well as all of their services and policies—including firewall, all types of VPN tunnels, routing tables, interface tables, network configuration, bandwidth and packet filters—can be made totally visible.

Unlike other VPN implementations, Cosine's IPSX switch gives each customer their own VR for each site, with all the capabilities of a standalone physical router. All of the customer's routing tables and routing polices are contained within their VRs, and the customer's physical interfaces connect to their own VR. The customer's interfaces are therefore called virtual interfaces. In addition, the customer's VR forms the basis of their VPN—and all services and policies, such as firewall services, bandwidth policies, etc.—are activated on their VRs.

The breadth and depth of the InGage CNM configuration reports—providing views at the network level, the tunnel level, inside the VR, connectivity to and from the VR and inside the firewall—provide a full picture of the customer's VPN in one easily accessible system. With this information at their fingertips, each enterprise customer, as well as your staff, can readily determine that all firewall, tunnel, routing, interface, and bandwidth policies and configurations are up-to-date, behaving as expected and consistent across the entire enterprise. Not only does InGage CNM give the same visibility for each component of the managed service one would expect from its physical counterpart (e.g., a standalone router or standalone firewall device), but InGage CNM also makes it easy to view the entire enterprise-wide VPN across all its component services.



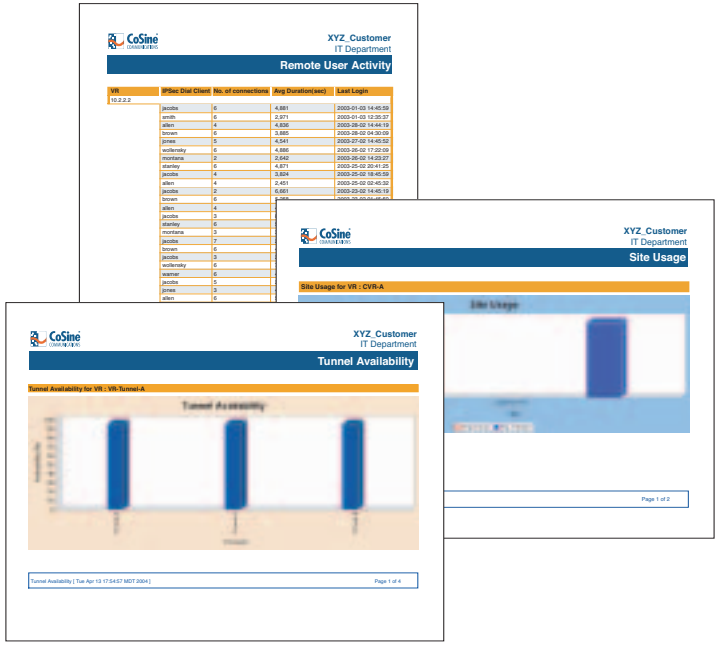
Configuration and Policy Details Across All Managed IP Services

Performance, Usage and SLA Reporting

With InGage CNM, enterprise IT managers can view granular usage, performance and SLA reports (comparing performance against pre-determined SLA thresholds) on all the components of their managed IP services, including:

- **Traffic and throughput reports** – inbound/outbound traffic for all types of VPN tunnels (e.g., IPSec, GRE and MPLS), as well as physical links and sites.
- **Firewall usage reports** – firewall sessions, firewall sessions by application type (e.g., FTP, telnet, HTTP).
- **Availability reports** – on all types of VPN tunnels, as well as sites, firewall and VRs, including reachability status of each VR and status of each physical and virtual interface on each VR.
- **Remote user activity reports** – number of connections, duration, and last login per user—for all dial and off-net remote users.

Armed with access to this level of detail, each enterprise customer, as well as your staff, can pinpoint problems quicker, make more informed planning decisions, implement preventative programs based on trend analysis and compare performance against SLAs. For example, you can determine if connections to certain hosts or destinations are available, which is a critical tool for resolving routing problems. Routing table reports can be used to determine how mission critical traffic is being routed over the VPN to another site or out to the Internet, regardless of whether the VPN is a mesh, star, or hub-and-spoke topology. In addition, InGage CNM provides storage of a rich range of usage data at the site, VR, tunnel, user and firewall levels, allowing innovative pricing plans.



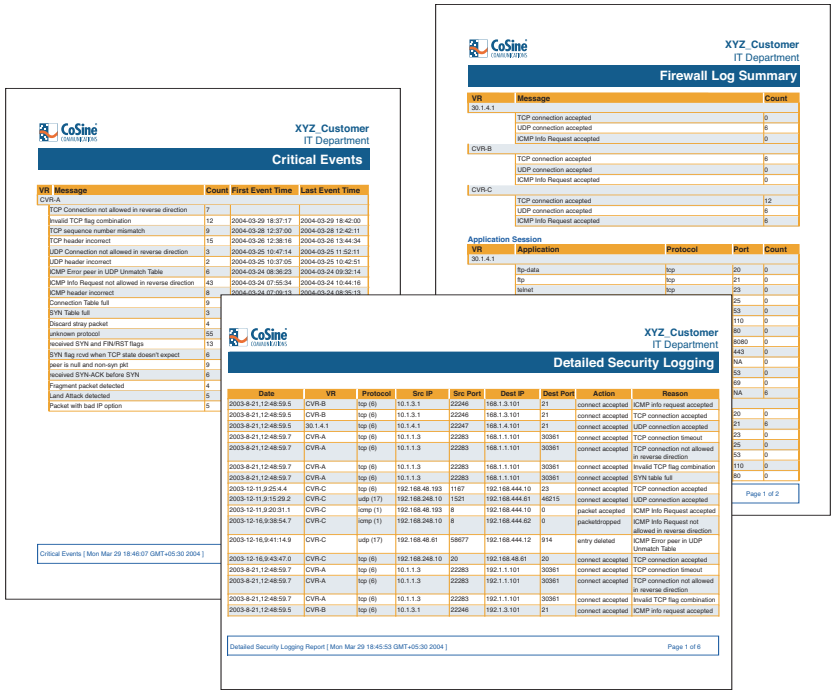
Analysis of Routing, Interfaces, Firewalls, All Types of VPNs and Remote Users

Firewall Activity Reporting

With InGage CNM, enterprise customers gain in-depth reports on important activities and events occurring within their managed firewalls.

- **Detailed Security Logs** – capture all security events (action, reason) and session activity (source/destination IP address and port) for each firewall.
- **Critical Firewall Events** – describe important details about critical events, including description, frequency and the first/last time each event occurred.
- **Firewall Application Sessions** – track each application session (e.g., FTP, HTTP, telnet) that crosses each firewall at each site of the customer's network.

These reports enable enterprise IT managers to demonstrate to management the level of value the firewall service is adding by making visible attacks that were thwarted. The firewall reports are also critical for improved security analysis, as well as planning, management and enforcement of corporate-wide security policies.



Seamless Operations Integration

InGage CNM provides efficient, scalable, flexible per-customer reporting and control for network-based IP services—optimized for rapid integration into the existing operational environment.

Using Java technology, open standards such as SNMP and CORBA, and extensive APIs, InGage CNM is designed to easily slot into any operational environment and provide nearly unlimited functionality extensions. Unlike other systems, InGage CNM does not force you to use built-in proprietary customer portals for customer interaction, vendor-specific database systems to store data or vendor-specific Graphical User Interface (GUI) filters for report extensions. With InGage, the customer interface can be your customer portal or internal Web-based systems, or some other interface within the carrier's OSS—giving you tremendous flexibility in packaging these functions for customers and their own staff.

For example, you can deliver reports based on customer account strategies, either via your customer portal, through e-mail or hand-delivered by account teams in face-to-face meetings. Data collection frequency, with a default setting of five-minute intervals, is configurable for each customer and each customer's service, as are the reporting frequencies (e.g., daily, weekly or monthly).

Rather than forcing you to use proprietary database systems, with the associated complexity of matching software revisions or proprietary report extension tools, which limit functionality, InGage CNM stores its data as parsable, structured XML. This XML data store not only simplifies report extensions but also makes them totally flexible, so there are no artificial constraints on report generation. XML also makes porting per-customer data into the carrier's OSS, billing and business intelligence systems for data-mining purposes very simple. In addition to report extensions, the rich set of APIs implemented in the InGage CNM means you can readily add nearly any customer self-management function you would like to offer (e.g., self-provisioning of bandwidth, firewall policies or adds/moves and changes).

Rapid Insight into Critical Firewall Activities for Security Auditing

COSINE INGAGE™

InGage CNM Architecture

The InGage CNM architecture, which includes the InGage CNM system working in conjunction with IPSX IP service switches and the InVision Service Management System (SMS), was optimized specifically for the level of rapid integration and efficient delivery needed to make CNM feasible in a carrier's environment:

- Layered, inherent per-customer architecture to protect each customer's data, as well as your control network
- Efficient network-based, per-customer data collection
- Open architecture for maximum flexibility, as well as rapid integration into your unique operational environment

The InGage Server is at the heart of the CNM architecture. The InGage Server dynamically collects per-customer data stored in the IPSX switches and the InVision SMS. The InGage Server then generates per-customer outputs in two forms (pre-defined Adobe Acrobat reports and XML structured data) and stores this per-customer formatted data in the InGage Repository.

InGage CNM handles all the interaction with the data collection points (InVision for configuration data, IPSX switch SYSLOGs for performance, usage and event data). Unlike other systems, which tightly bundle the customer interface giving customers direct access to the carrier's policy server and provisioning system, InGage CNM intentionally unbundles these functions. The customer interacts only with your customer interface, which handles authentication of the request and distribution of the reports. This layered architecture presents a clear demarcation point between the customer and your infrastructure.

In addition, the entire CoSine architecture—the IPSX switches, the InVision SMS and the InGage CNM—is structured from the ground up on a per-customer, per-VPN basis, so each customer's VPN is completely disjoined from all others. This separation at the switch, provisioning system and CNM levels, means that each report is generated and stored on an individual customer basis, ensuring that each customer has access to only their VPN.

Further, since the entire CoSine IP services delivery platform is structured from the ground up to deliver network-based services on a per-customer basis, the InGage CNM data collection functions are inherently efficient and scalable. This process eliminates the need for thousands of software agents, hardware probes, and complex tiers of collectors, aggregators and reporting servers.

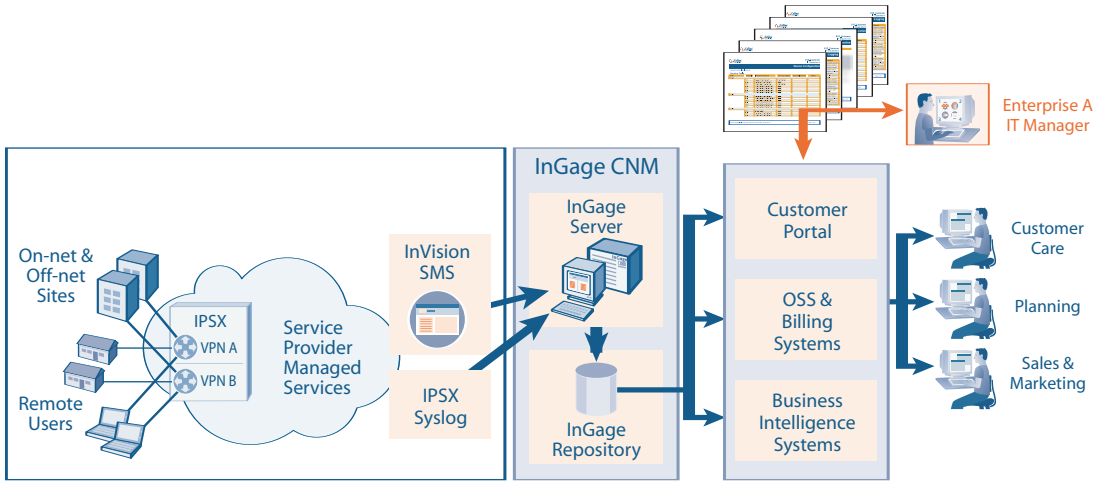
System Requirements

InGage Server

- Solaris™ based hardware per Fujitsu specifications such as Fujitsu PrimePower® servers
- Sun® Solaris™ 2.8
- Oracle® 8.1.7 (license included)
- 2 GB RAM (minimum)
- 10 GB hard drive (minimum)

InGage Client

- Any platform that can support the Microsoft Internet Explorer, Netscape or Mozilla web browsers



Fujitsu Network Communications Inc.

2801 Telecom Parkway, Richardson, TX 75082

Tel: 800.777.FAST Fax: 972.479.6900

www.fujitsu.com/us/telecom

COSINE-INGAGE/DS/1.0/06.04/CM