

Sun and Bridgewater Systems Network Access Control Architecture

Building a secure carrier-grade infrastructure



Today's carriers often serve as many as 70 million customers and must support a growing variety of user devices and applications across multiple networks. It has thus become a major challenge to provide secure access control while keeping costs low and enabling business agility. Today's carriers require a secure carrier-grade infrastructure that can support cost-effective business growth and simplify subscriber management, so that new services can be deployed quickly and easily. Sun and Bridgewater Systems have defined a joint solution that provides a highly secure foundation and enables rapid deployment, management, and monetization of IP services in the telecommunications infrastructure.

Highlights

- Subscriber-centric policy management on a highly secure carrier-grade infrastructure
- Performance and scalability to support business growth
- Rich subscriber experience based on a unified subscriber-centric view of information
- High-performance network access control using cryptographic acceleration built into the UltraSPARC® T2 processor
- Entitlement control that combines sophisticated network and application policy to manage subscriber authorization to network resources and applications
- A single common repository for managing both subscriber profiles for carrier services and user profiles for enterprise applications

New opportunities with IP services

Next-generation networks and the IP Multimedia Subsystem (IMS) empower carriers to offer interactive, multimedia-enabled, IP-based sessions that can be delivered over any device, on any access network — including wireline, 3G, WiMAX, and LTE networks. This gives customers the capability to use multimode wireless handsets on an enterprise Wi-Fi network while at the office, and then to continue the conversation by shifting onto a cellular network when leaving the premises — all with a single, continuous session and uniform quality of experience. These sessions provide access to all of the telephony services available today, as well as supporting a new class of IP-based services available over the Internet. Next-generation networks enable carriers to create new types of services that integrate voice, video, text, content, and presence as part of the service mix, regardless of the access technology.

These new services offer an opportunity for communication carriers to extend their reach into new markets and to deliver services to customers over networks that are beyond their direct control.

Managing complexity in the network infrastructure

Next-generation services can potentially create a need for yet another repository to be added to the long list of databases that wireless and wireline carriers must synchro-

nize and maintain. Today's communication carriers struggle to maintain consistent, up-to-date databases for customer billing, service provisioning, customer relationship management, and session management. When carriers add new customers, they often must add entries for them in all of these databases. If customers change service plans or preferences, a carrier's business processes must also coordinate these changes across the entire range of affected databases without introducing inconsistencies, security vulnerabilities, or revenue leakage. Worse yet, when a carrier adds new services, sufficient information to provision, support, and bill for them must be added across a range of systems, making it difficult, costly, and time-consuming for carriers to branch out into new markets.

By establishing a common user repository to manage subscriber entitlements for all IP services, carriers can greatly simplify the management of subscriber profiles and thereby reduce security vulnerabilities while also enabling greater business agility and decreasing operational costs.

Sun and Bridgewater Systems network access control architecture

Sun and Bridgewater Systems have combined forces to deliver subscriber-centric policy management on a highly secure carrier-grade infrastructure. A subscriber-centric policy decision point provides the

foundation for rapid deployment, management, and monetization of IP services. The combined solution not only simplifies the task of managing subscriber policy but also provides a highly secure and scalable carrier-grade infrastructure. The primary business benefits:

- Easily and quickly deploy new profitable services
- Increase average revenue per user (ARPU) and improve subscriber retention
- Control and deliver a rich dynamic subscriber experience
- Support scalability for business growth across wireline, 3G, WiMAX, LTE, and converged networks
- Reduce operational costs through a more efficient carrier-grade infrastructure and simplified subscriber management

Bridgewater Systems

The Bridgewater Systems product suite enables carrier services to build a unified view of the subscriber in real time by easily gathering data from multiple sources. Subscriber data management is a core, underlying capability across all Bridgewater products to bring subscriber context to policy decisions. Subscriber information — such as static profile details related to entitlements, dynamic real-time state information, and subscriber history (both static and dynamic) — is integrated into a subscriber-centric policy decision point. Bridgewater Systems has two product categories that work together to control access to all networks and services on a per-subscriber basis.

Network access control

The Bridgewater Systems network access control solution enables carriers to deploy centralized authentication, authorization, and accounting (AAA) functions, as well as IP address management, across multiple access networks. The AAA Service Controller is designed for multivendor environments and offers dual RADIUS and Diameter support to control access across an array of access

Network access control

High-performance authentication, authorization, and accounting; IP address management; and IMS subscriber repository

Entitlement control

Control, monetize, and enrich subscriber interaction with applications and network resources

Subscriber data management

Robust real-time subscriber session management

Figure 1. Bridgewater Systems provides a centralized approach to controlling access to all networks and services on a per-subscriber basis.

technologies for wireline, 3G, WiMAX, and LTE networks, as well as a migration path to IMS frameworks.

The Bridgewater Systems Home Subscriber Server extends network access control by offering a high-performance platform for maintaining IMS subscriber profiles, registering devices, and monitoring session activity in real time.

Entitlement control

Carriers can control and monetize the dynamic entitlement relationship among subscribers, applications, and network resources using the Bridgewater Systems Application Policy Controller and Network Policy Controller.

The Bridgewater Systems product suite eliminates duplicated infrastructure and service silos that can increase cost and complexity. With subscriber-centric policy management, carriers can create highly flexible policies tightly aligned to business needs and subscriber entitlements, which helps improve subscriber retention and increase ARPU.

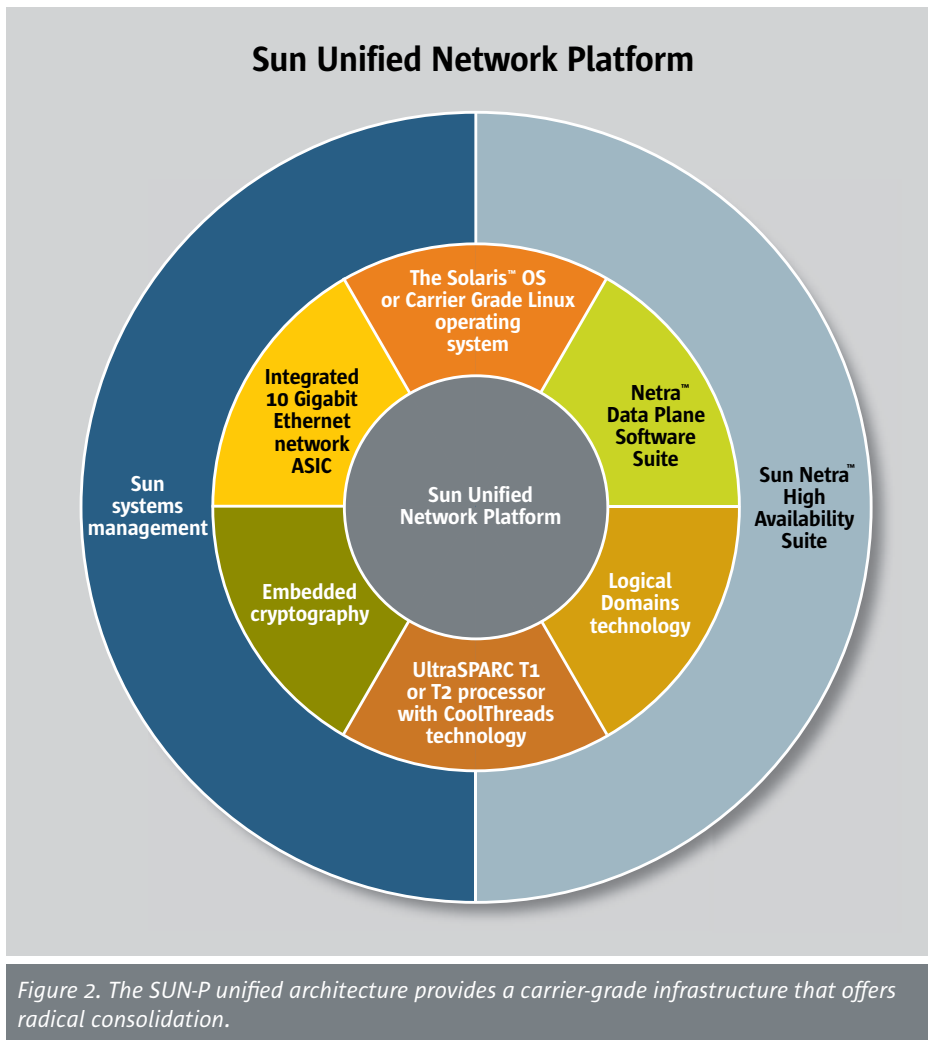
Sun™ Unified Network Platform

The Sun Unified Network Platform (SUN-P) offers a radically consolidated, scalable core network architecture based on a new generation of multicore/multithreaded processors. It provides a new approach to building the core network infrastructure, enabling telecom carriers to significantly reduce the cost to serve the first subscriber while providing massive scalability for network expansion.

Unlike traditional network architectures that are built using proprietary systems, the SUN-P architecture is based on open standards and commercial-off-the-shelf (COTS) components, as shown in Figure 2. This provides a simplified development and deployment environment that can help reduce costs and increase business agility.

The SUN-P architecture enables carriers to benefit from:

- Radical cost savings, as a result of eliminating the need for physically separate servers for every network element



- Faster time to market, due to greatly simplified application development versus proprietary platforms and technologies
- The ability to start small and grow to millions of subscribers on the same hardware and software architecture
- Investment protection through a scalable, open architecture solution

These benefits are made possible by recent technology advances from Sun in the areas of chip multithreading (CMT) technology, machine virtualization, and high-performance networks, as described in the component description sections that follow.

The network access control architecture includes the Bridgewater Systems product suite deployed using the SUN-P architecture, and it utilizes Sun technologies to further enhance security and increase efficiency. Figure 3 shows a logical description of the architecture and identifies the specific Sun technologies that apply to each of the three functional areas of the Bridgewater Systems product suite.

Specific advantages of this architecture include:

- Increased security, with an entire carrier-grade infrastructure that takes advantage of the security features in the Solaris 10 Operating System (OS)

- High-performance AAA, using built-in encryption in the UltraSPARC T2 processor to accelerate packet processing for encrypted data
- Increased flexibility and reduced compliance risk, with the help of the optional integration of Sun Java™ System Identity Manager to more efficiently manage entitlement control in a highly distributed environment
- Simplified subscriber management with optional integration to the Sun Java System Directory Server, enabling carriers to manage their subscriber profiles using the same repository that is used for their enterprise applications
- Modular architecture, which enables carriers to add ancillary features easily and to integrate best-of-breed functions within the same platform
- Cost-effective, consolidated solutions using Sun Logical Domains (LDoms) and Sun Netra ATCA CMT blades in the SUN-P architecture

The specific components of the architecture are further described in the following sections.

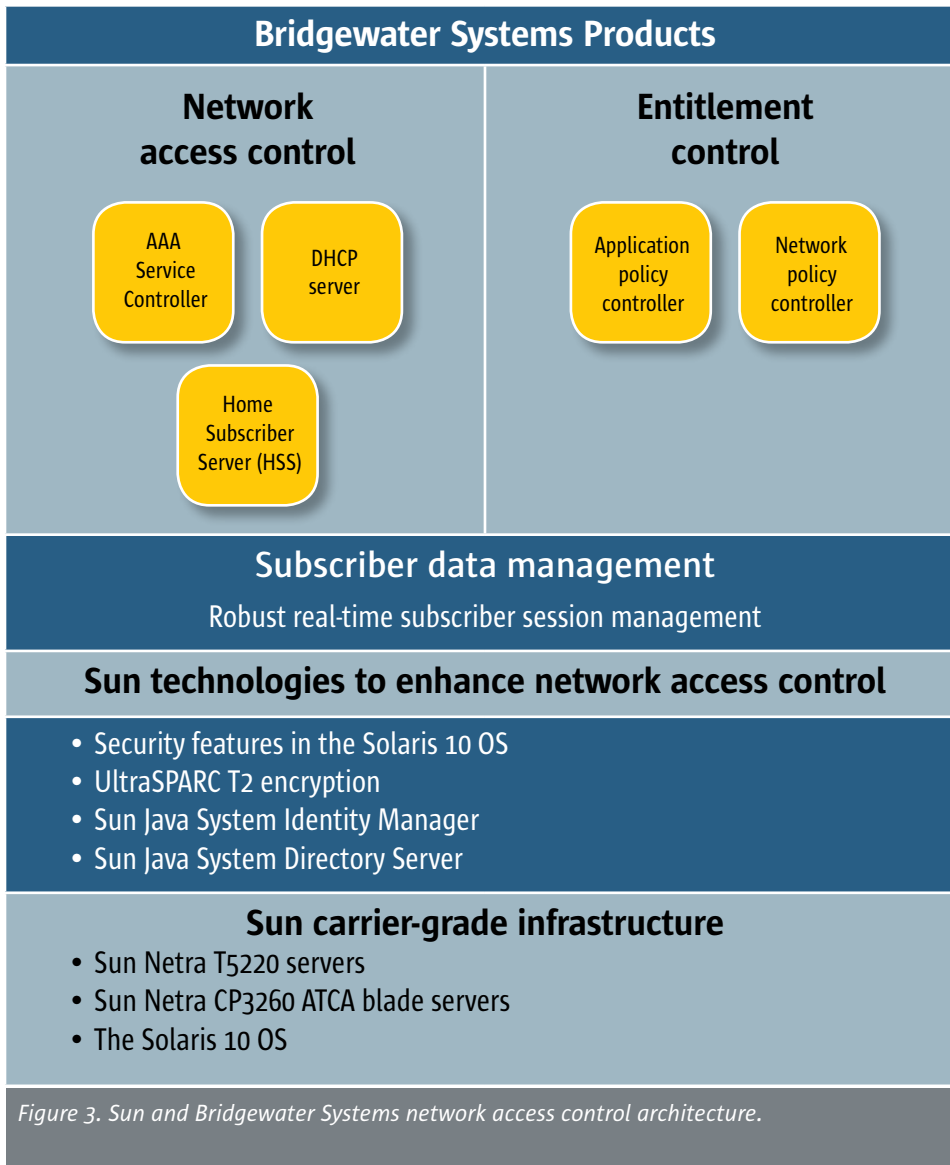
Bridgewater Systems AAA Service Controller

The Bridgewater Systems AAA Service Controller is the most proven, scalable, and robust solution of its kind. Built around a powerful policy and profile engine, the AAA Service Controller enables carriers to offer and control access to advanced and differentiated services across all access types and infrastructures. The open distributed architecture delivers the power to define and manage subscriber policies, and profiles centrally while extending local control to business or retail customers.

Bridgewater Systems Home

Subscriber Server

The Bridgewater Systems Home Subscriber Server (HSS) enables access to the master repository that maintains information for the authentication, authorization, and



establishment of subscriber calls and sessions. This includes support for SIP-based applications such as video sharing; RADIUS interfaces to the PDSN, GGSN, and HAs; and Diameter interfaces from SIP applications. In addition, the HSS holds significant subscriber profile information and can be deployed with the Sun Java System Directory Server to create a single enterprise repository for both subscribers and application users. Subscriber information can be delivered to an application on demand, or as the subscriber information changes.

The HSS includes built-in redundancy and high reliability to help ensure five-nines (99.999 percent) availability, and it is fully integrated with the Bridgewater Systems AAA Service Controller. It is available as a standalone HSS and operates in multi-vendor networks.

Bridgewater Systems Network Policy Controller

The Bridgewater Systems Network Policy Controller provides comprehensive network

policy control in IMS and next-generation network environments. Carriers can create their own customized business rules that simplify policy enforcement. Business rules are based on both static and dynamic information including subscriber profiles and preferences, current network resource allocation, and the status and characteristics of available applications. Additionally, the Network Policy Controller incorporates the standards-based Policy Control and Rating Function (PCRF).

Sun Netra T5220 server

Optimized for carrier-grade networks, the Sun Netra T5220 server is the first NEBS Level 3-certified rackmount server to integrate 10 Gigabit Ethernet (GbE) technology directly from the system processor. It also features the industry's most ruggedized enclosure, which provides a high level of system reliability and availability. The server supports large workloads, with up to 64 GB of memory. It also provides hardware RAID 0 and RAID 1 support for the pair of internal hard drives.

Sun Netra CP3260 ATCA blade server

An important part of Sun's continuing commitment to CMT-based computing for telecom, the Sun Netra CP3260 ATCA blade server is a second-generation CMT-based telecom blade that meets ATCA standards. The server has industry-leading memory capacity with eight memory sockets, and offers a disruptive leap forward in ATCA blade performance. It has a balanced I/O architecture through the use of new, advanced rear transition technology, which provides high-speed Zone 3 connectivity solutions and 10 GbE ATCA extended fabric support. This high-performance, compact server delivers extremely high compute density per shelf.

UltraSPARC T2 processor

The UltraSPARC T2 processor is the industry's first true "system on a chip," packing the most cores and threads of any general-purpose processor available. It integrates all the key functions of a server on a single chip: computing, networking, security, and I/O.

With up to eight multithreaded cores and 64 simultaneous threads, the UltraSPARC T2 processor improves throughput while using less power and dissipating less heat than conventional processor designs. It provides massive scalability by executing eight threads per clock cycle using CMT technology. This enables carriers to execute all types of workloads at very low power. It also includes integrated 10 GbE support as well as integrated floating-point and cryptographic processing in each CPU core, to enable extreme throughput.

Secure virtualization with LDom technology

Sun's LDom technology is built in as standard to the UltraSPARC T1 and T2 processors, enabling carriers to deploy one of the industry's most open virtualization solutions with no additional licensing costs. LDom enable consolidation of the carrier-grade infrastructure by dividing a Sun server or ATCA blade into multiple logical servers.

LDom technology provides a lower cost structure for initial subscriber offerings by enabling each LDom to start small and then increase its resources whenever throughput and capacity requirements change. Each network element runs in its own virtual server with its own OS instance and its own memory, I/O, and computing resources.

Improved security with the Solaris 10 OS

The Solaris 10 OS is the current version of Sun's tested, certified, and supported enterprise OS, available free for download. The strong industry reputation for the security and reliability of the Solaris OS is based on many years of engineering investment from Sun.

The Solaris 10 OS includes significant features that can help prevent unauthorized access to data and applications:

- Role-Based Access Control (RBAC) provides strict control over the access rights that both users and applications can exercise
- Process Rights Management, a feature that was once available only in the Trusted Solaris™ product, further restricts access by preassigning access rights to user processes, significantly limiting the damage that can be done if the process is somehow compromised by an attack
- Solaris Cryptographic Framework provides a mechanism and API whereby both kernel- and user-based cryptographic functions can transparently use hardware accelerators such as those in the new UltraSPARC T2 processor
- The Solaris Security Toolkit, formerly known as the JumpStart Architecture and Security Scripts (JASS) toolkit, provides a flexible and extensible mechanism to harden and audit the Solaris OS
- IP Filter software protects systems running the Solaris 10 OS by limiting the type and direction of network traffic flowing to and from a system. It can be used to easily enable a system to access the resources it needs on the network while limiting what network services are exposed by the system

These security features in the Solaris 10 OS can also be easily extended, due to the open-standards approach that enables third-party security solutions to be integrated into the Solaris security architecture.

Sun Java™ System Identity Manager

Sun Java System Identity Manager can optionally be integrated with the Bridgewater Systems product suite to give carriers additional capabilities that can reduce the cost of provisioning subscriber profiles and help decrease compliance risk. It provides comprehensive user provisioning and identity auditing for efficiently and securely managing identity profiles and permissions across the enterprise and beyond.

Sun Java System Directory Server Enterprise Edition

Sun Java System Directory Server Enterprise Edition can optionally be integrated with

Learn More

For more information about the Sun and Bridgewater Systems network access control architecture and related technologies for telecom, go to:
sun.com/wimax
 or sun.com/netra

the Bridgewater Systems product suite to provide a single common repository for both the Bridgewater Systems Home Subscriber Server solution and enterprise applications. Sun Java System Directory Server is a high-performance enterprise directory server that provides excellent scalability for carrier-grade infrastructures. It provides all of the essential data services including proxy and virtual directory, and includes data distribution to provide a highly available directory service.

Build a secure infrastructure with Sun and Bridgewater Systems

Today's increasingly complex and distributed networks, and the growing subscriber bases they serve, demand a new approach to security and subscriber management. The Sun and Bridgewater Systems network access control architecture can provide a highly secure and cost-effective method for delivering new 4G services to subscribers. The architecture offers a radically simple approach to maintaining subscriber data and building out the carrier network. This simplicity translates into faster time to market for new services and dramatic reductions in operational cost — all while delivering industry-leading security.

The Sun and Bridgewater Systems network access control architecture can also be combined with Sun Services offerings that can help carriers accelerate deployment and get the most value from their investments. Specific configurations might also be available through the Sun Customer Ready program.

