NEWNET PRODUCT BRIEF

AccessGuard 1000

Secure IP payment transaction accelerator for routing and switching millions of transactions per hour

OVERVIEW

Internet protocol has proven itself to be the enabler behind a varied range of communication conveniences that we take for granted. It clearly has established itself as the de facto standard for transmitting data over the internet. It is also a key element in the realization of ubiquitous wireless broadband. Emerging trends, such as electronic payment processing and the move to making commercial transactions less dependent on using cash are based on IP.

Globally, electronic transactions have increased globally in volume and dollar value over the previous years and continue to grow. Worldwide e-commerce spending is estimated to exceed $1 Trillion in the next few years and over 12.5% of all e-commerce transactions will be conducted over smartphones soon. Close to $1 Billion handsets with contactless capability including NFC etc. is expected to be in use in the next few years and it is estimated that significant proportion of all POS terminals will have contactless capability in the same timeframe. All these estimates point toward a huge increase in mobile, broadband IP transactions, which is expected to cross over $45 Billion transactions and be, valued over $10 Trillion in the next few years.

This IP based 21st century payment system network architecture is driving payment processing and the industry is seeing a convergence of mobile and broadband IP-centric products and services. Increasingly, more financial institutions, insurance companies and businesses around the world are using the mobile and broadband internet to offer products and services and enhance an expanded suite of communications based services to its consumer's customer base. Internet based transactions have many obvious advantages over traditional telephone line based transactions. These include the potential to reduce the transaction costs, improve transaction time, and an increase in the payload size is regarded as a major driving force for financial institutions to switch over to the internet.

All this progress does not come without concerns. Since the mobile, broadband internet is a public network and the basic IP protocol lack the most basic mechanisms for security, such as authentication, message integrity, and data confidentiality, the network infrastructure that Financial institutions choose must have uncompromised performance, be highly secure and safeguard the information it collects in order to avoid a security breach and costly surprises.

The solutions from NewNet deliver fundamental security capabilities to enable safe and effective means of conducting financial transactions, data collection, security verification and custom applications over the internet any day, any time.

This application brief focuses on how existing legacy and new generation bank host systems are interconnected to the mobile, broadband internet based Point of Sales (POS) terminals, ATMs, NFC Terminals, smart phone and Tablet based mobile payment terminals etc, for the next generation financial transaction market.

NewNet
SECURE PAYMENT TRANSACTIONS

NFC Mobile Wallet Payment Routing & Mobile Payments

Global mobile subscriber base is expected to touch 6 billion in the near future. Mobile phones have advanced far ahead from being a basic voice communication device to a multi-purpose device with an appealing form factor which enables internet access, streaming videos, multimedia messaging, discount coupons, airline check-ins, mobile banking, mobile payments and even as a true mobile wallet. With the expanding payment application capabilities on the mobile phones combined with the huge subscriber base that could potentially avail these services, the mobile carriers are identifying the vast opportunity for mobile payments and mobile commerce (m-commerce).

Several of the mobile carriers, acquirers, processors and service providers in different geographies are making entry to the electronic payment transaction segment in several different ways offering multitude of services and many more carriers will follow soon. The service models continue to evolve and are expected to continue to expand with different geographical regions preferring certain select services to the other. Security remains a major concern for all these services, increasingly because many of these are employing innovative ways of doing transactions and involves newer levels of security requirements to handle the fraud associated with these new services.

The payment industry requires processing platforms with interfaces to multiple data access nodes and servers. A mobile carriers' network must have the latest, advanced and strongest security procedures and capability to handle the mobile transactions using a variety of protocols. These Carriers are deploying industry proven applications for transaction processing and edge routing, Mobile carriers or merchant acquirers are offering a unique range of services across mobile merchant POS terminals for NFC Mobile wallet payments and Mobile POS transactions.

As usage of the Internet both over broadband and mobile for business and financial transactions increase, their lack of built-in security has become more and more problematic. Additionally, global mobile subscriber base is expected to touch 6 billion in the near future. Mobile phones have advanced far ahead from being a basic voice communication device to a multi-purpose device with an appealing form factor which enables internet access, streaming videos, multimedia messaging, discount coupons, airline check-ins, mobile banking, mobile payments and even as a true mobile wallet. The volume of transactions, once these mobile devices could be enabled to make mobile payment transactions is estimated to be huge in the years to come.

NFC technology is fast driving the emergence of mobile POS terminals with the ability to enable mobile wallet payments with increased potential to avoid card swipe based transactions in the longer term and save the consumer from carrying multiple payment cards in the wallet. For these transactions, security becomes an even bigger concern to ensure that all electronic information related to payment cards is safe and transported securely.

Any security product portfolio for financial services over the internet should address the following fundamental security issues:

- Authentication (person's identity is ensured)
- Authorization (person is allowed to have access to data)
- End-to-end Encryption (data confidentiality)
- Digital Signatures

NewNet
SECURE PAYMENT TRANSACTIONS

In addition to the fundamental security services, in depth knowledge of each transaction application may be critical in order to provide a cost effective solution. For an example, in Point of Sales (POS) networking, it is common for some of these systems to require specific standards and protocols implementation and customization. Due to this, a generic product that provides only internet security may not be suitable for all financial transactions.

When evaluating systems for transaction processing, financial institutions will look for which technology or solutions best suit for their needs. When replacing the existing system with new technology, Financial institutions must evaluate interconnecting and integrating their existing system with new services. There is a significant business risk and costs associated with just simply discarding the legacy system and replacing it with a brand new system. For example, in financial transactions where legacy hosts work on X.25 network moving the transactions to over the internet requires the host server to support all the security requirements of a next generation IP infrastructure.

Other challenges include adding scalability and redundancy without sacrificing overall performance. Security transactions include cryptographic encryptions, which will impact the CPU performance, limiting the number of transactions and response time required.

NewNet's Security Solutions for Payment Processing

Secure Socket Layer (SSL) / Transport Layer Security (TLS)

SSL/TLS is a cryptographic protocol that provides secure communications over the internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. SSL involves a number of basic phases:

- Peer negotiation for algorithm support
- Public key encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

Encryption

The most widely used encryption algorithms for SSL are AES, 3DES and RC4.

Advanced Encryption Standard (AES): Advanced specification for the encryption that supports 192, or 256 bits.

Triple DES (3DES) : Encrypts messages three times using DES 56-bit key, which is effectively 168-bit key encryption.

RC4 : Stream cipher developed by RSA Data Security, Inc. key-length is variable but typically used is 128-bit.

Key Exchange Algorithm

Symmetric key cipher requires a key to be used to encrypt the communications. When two parties have no prior knowledge of each other, they must jointly establish a shared secret key for encryption over an insecure communications channel.

The most widely used algorithms for exchanging or generating shared key at both ends of the communications link are RSA and Diffie-Hellman. Diffie-Hellman is a key agreement protocol, where the algorithm generates a shared secret at both ends of the communications link. RSA is a public-key cipher, which works as a key transport protocol, by which the algorithm sends out a secret key to the other end of the communications link.

SSL Acceleration

SSL acceleration is a method of offloading the processor-intensive public key encryption algorithms involved in SSL transactions to a hardware accelerator. The SSL Accelerator solves the problem of server (host) slowdowns caused by running SSL in software using the host CPU. Typically, this is a separate co-processor, specifically designed for handling encryption algorithms using parallel processing at very high speeds.

SSL Offloading

SSL offloading may look very similar to SSL acceleration. The term “offloading” is generally used to describe a completely separate computer that performs all SSL processing, so that the SSL load is taken off of the server completely. In a sense, an SSL hardware accelerator is performing SSL offloading, because part of the SSL processing is “offloaded” from the server’s CPU to the hardware accelerator. An advantage of an offloader, as opposed to the typical accelerator, is that it can perform SSL processing for more than one transaction server, whereas the accelerator card is tied to a single server.

Digital Certificate

Key agreement or key transport schemes are vulnerable to man-in-the-middle attacks. A solution to this problem is to send the public key over the communication link using a signed certificate.

A certificate is a document that contains, along with the public key of the sender, the name of the certificate holder as well as the digital signature of an independent and trusted third party, called certification authority (CA), to ensure the validity of the transmitted information. The certificate format is usually based on ITU-T recommendation X.509.

During SSL negotiation, certificates are exchanged for public key information. These certificates are validated with CA. Upon validation; this public key is used for shared key generation for symmetric encryption.

Addressable Markets

Internet security is fundamental and necessary to the successful adoption of the new economy and markets such as Internet Banking, internet commerce, mobile banking, mobile commerce, mobile wallet payments, e- governance, and medical records. NewNet‟s security solutions can be used in the following markets to provide secure financial transactions, data collection and custom applications over the internet.

Airline

- Reservations

Financial

- Electronic fund transfer (EFT)
- Electronic data interchange (EDI)
- Electronic benefits transfers (EBT)
- Electronic trade confirmations (ETC)

General

- Data collection
- Custom applications

Health

- Medical Records transactions

Insurance

- Data collection

Security

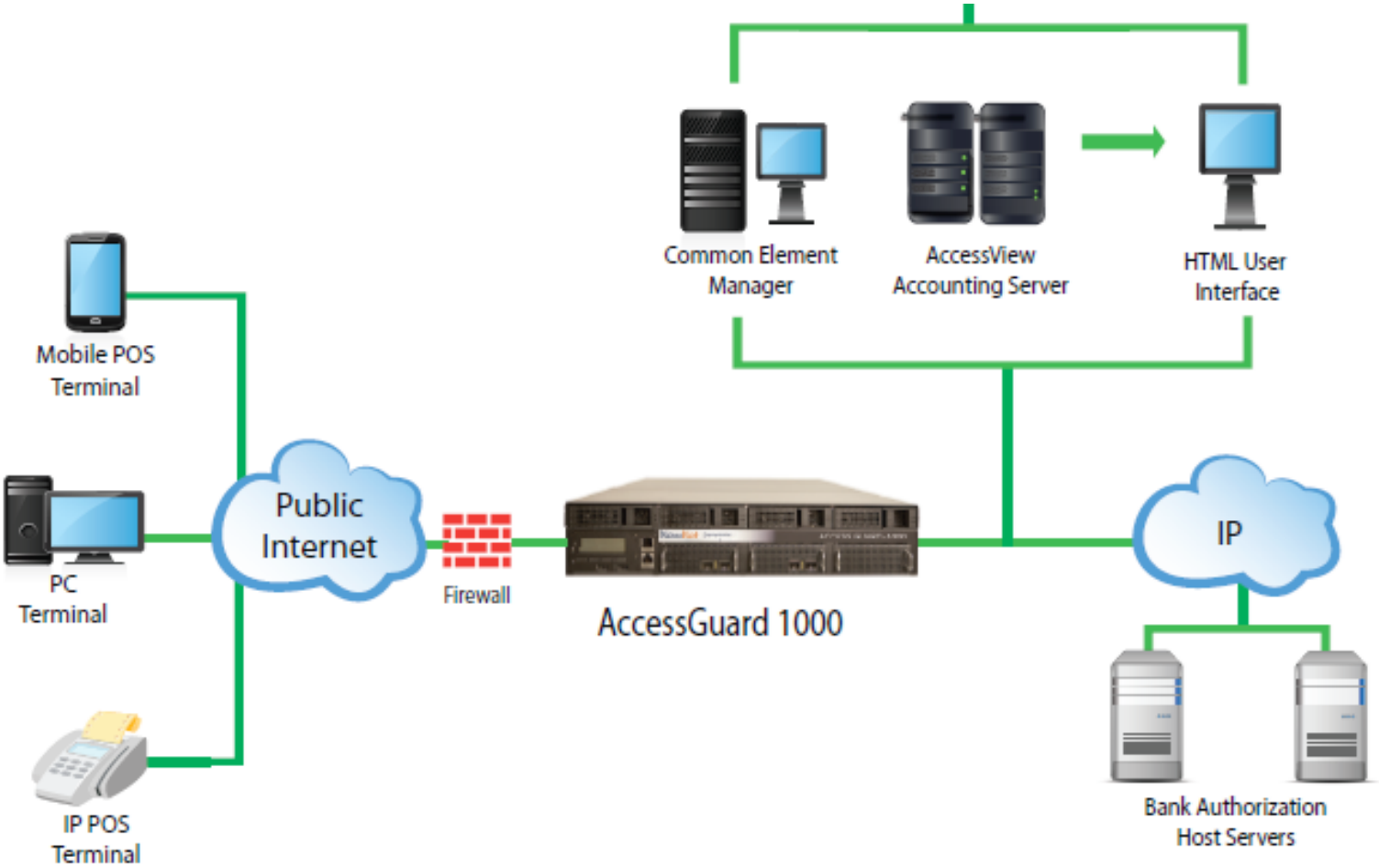
- Pin encryption and verification for transactions
- ID verification
- Security verification

NewNet
SECURE PAYMENT TRANSACTIONS

AccessGuard 1000 Mobile/Broadband Payment Gateway

Traditionally, POS based transactions are initiated by POS devices dialing into the PSTN, which then transfer data via standard V (modem modulation standards V.32, V.90, V.x), series modulations using VISA I, VISA II and similar protocols. As the industry moves to all IP architecture and POS devices convert to mobile or broadband IP only devices, the need to aggregate and securely transport this information back to a central server is required. The NewNet AccessGuard 1000 is designed to meet this specific market, as it will provide a secure means of connecting mobile or broadband IP POS devices, mobile data devices like Tablets and smart phones with card readers etc and securely transporting the information to hosts over the insecure internet.

In this next generation network, a merchant has one or more mobile, broadband IP enabled POS devices sharing a high-speed public internet link (Wireless, Cable, or DSL modem). AccessGuard 1000 supports transaction protocols like VISA I, VISA II, ISO 8583, TPDU (Transport Protocol Data Unit), and Custom Protocols, which expedites the financial transactions. AccessGuard 1000 terminates SSL sessions that are originated from the IP supported POS. In this model, the acquiring bank host system continues to operate in the same model as it was operating with the legacy transaction mode.



NewNet
SECURE PAYMENT TRANSACTIONS

AccessGuard 1000 brings :

- Cost reductions of transactions
- Security to the insecure IP POS terminals
- Interconnect the legacy bank host computer with the next generation IP POS terminals
- Aggregate the connections for saving host's resources.
- Simplified solution
- CAPEX savings to avoid hosts replacement using the public internet
- Safeguard sensitive credit card data over the public internet
- Offer opportunity to provide more value add services
- Faster transactions using state if the art hardware accelerator
- Highly scalable for location based growth
- Redundancy for network disasters: record recovery
- Integrated platform for broadband internet and mobile payment transaction processing

Mobile Payment Processing

AcessGuard 1000 offers a wide variety of service options for enabling multiple types of mobile payments, mCommerce and mobile wallet services.

The supported mobile payment interfaces on AG1000 includes;

- Mobile browser based payments
- Mobile application based transactions
- SMS/USSD based payments

AcessGuard 1000 inter woks with these payment methods by interfaces to SMS/USSD gateways and HTTPS interface to the mobile device for the mobile browser or mobile application based transactions. These payment transactions from mobile devices are processed on the AccessGuard 1000 and sent to the banking or financial institution servers for the payment approvals and authorizations.

AcessGuard 1000 seamlessly enables the payment transactions for the two broad mobile payment service categories which are the retail merchant location based mobile POS based payment transaction and subscribers‟ mobile device initiated mobile wallet based payments.

Key Features and Benefits

Feature	Description	Benefits
Transaction Protocol Support	The AG1000 is specially designed for the POS industry and supports all major transaction protocols - VISA I/ II - TPDU, ISO 8583 - HTTP transactions - XML protocols	The support of all major transaction protocols and capability to interwork these ensures interoperability between the hosts and POS terminals. As opposed to other solutions that look at the transaction protocols superficially, the AG1000 understands the transaction protocols. This enables the AG1000 to be used for providing intelligent applications using the transaction protocols.
Transaction Routing	Routing of transactions based on several mechanisms including specific fields in packet headers, payload fields etc like transaction NII in TPDU etc. The system has the capability to multiplex several transactions to host server on a single connection, which may be maintained as persistent session.	The AG1000 ensures that transactions are sent to the correct destination. It also balances transactions to avoid congestion and bottlenecks and diverts transactions around known failures.
Secure Access	SSL 3.0, TLS 1.0/1.1/1.2 and IPsec. SSL, TLS and IPSec are cryptographic protocols that provide secure communication over the Internet.	The AG1000 solution can aggregate thousands of persistent and non-persistent SSL/TLS/ IPSec connections and transactions. AG1000 can also support sessions re- use, introduced in SSLv3, which is used to reduce the burden of establishing a new SSL session by reusing previously established SSL Session ID's.
Network Routing	The AG1000 supports the suite of routing protocols RIP, OSPF and BGP-4.	The support of routing protocols helps network administrators configure IP routing in the network to maximize system availability.
Load Balancing	Distribution of traffic to Host servers based on pre-defined criteria for sharing the load in a proportionate fashion. The load balancing criteria include default mechanisms of round robin, pre-defined preference values, outstanding traffic or active load, ability to process transactions swiftly or response delays etc.	This can be applied on multiple Host servers configured in a Host group, or destinations defined for specific packet traffic. Additionally this can be combined with the routing protocols to ensure the traffic is distributed across the available paths.
Virtualization	System supports the ability to segregate traffic into traffic groups and then have the ability to reserve resources for those traffic groups. The segregation of traffic into groups can be done on the basis of traffic type like HTTPS, SSL, transaction types like TPDU, ISO8583 or other parameters like Local IP address/port, remote IP address ranges, VLANs, etc. The system allows the configuration of percentage of system resources that shall be dedicated to each traffic group. This ensures that one traffic group does not starve other groups and a fair distribution of system resources is maintained. Associated user groups can be assigned which restricts users to be allowed to access the specific traffic group related configurations only.	This capability ensures the logical virtualization of the system enabling acquirers, processors and carriers to offer differentiated services on the same systems to multiple customers by still maintaining complete isolation of capabilities and access controls exclusive to the respective traffic and service groups.
Certificate Status	AG1000 offers verification on client and server certificates and provides information regarding the certificate validity.	The certificate information can be listed and viewed and appropriate traps are generated when the validity expires or a configured.

Key Features and Benefits

Feature	Description	Benefits
PCI Compliance	- Build and Maintain a Secure Network - Protect and store Cardholder Data - Encrypt transmission of cardholder data across open, public networks - Maintain a Vulnerability Management Program - Implement Strong Access Control Measures - Restrict access to cardholder data by business need-to-know - Assign unique ID to each person with computer access - Restrict physical access to cardholder data - Regularly Monitor and Test Networks - Track and monitor all access to network resources & cardholder data - Regularly test security systems and processes - Maintain an Information Security Policy	AG1000 insists on password protection for all users accessing systems including password control for system consoles and remote sessions. System do not store any card data and all key information stored on systems are encrypted. All data transmissions are encrypted from and to the system. System access is restricted with access control lists and levels of access. All system accesses and configuration changes are logged and made available for audit trail. We build fail-safe model, which leaves no options for user to create non- compliant configurations avoiding security risks and offer fully compliant systems.
Group Monitoring	Systems has the ability to track and display the status of all Host servers in a group by indicating the tracked status being active or non responsive.	This information can be used for acting upon by the operators or NOC teams to restore the services of servers out of action.
System Utilization	Detailed information of system resources utilization including processing resources, memory, interface status, traffic volume for tracking and monitoring purposes.	System management teams can proactively utilize this information for service improvements and efficiencies.
Keep Alive Mechanism	Customized mechanisms for maintaining keep alive mechanisms between configured targets for status determination.	This feature is vital in ensuring the actual status to destination systems and making intelligent decisions on traffic re-routing.
Packet Filtering	Rules based packet filtering capability to filter traffic from avoidable sources or known/learned un–trusted sources. Packet inspections for known patterns or signatures for early action to drop these before further forwarding.	Protects systems from known internet vulnerabilities and increase additional security layer over and above external firewalls.
Authentication	Radius, TACACS, and LDAP based authentication	Variety of external authentication servers
DUKPT Encryption	AG1000 enables the terminal devices to offer advanced security capability for card data over and above the session security provided by the SSL/TLS protocols	Enhanced security for card data which will still be secure over and above the session security
Secure Shell	Access to the AG1000 is secured and authenticated via Secure Shell-2 procedures. Authorized clients can connect to the internet via Ethernet interfaces on the AG system.	All user access to the systems remains over secure access mechanism only
Configuration	Configure the system from the common management tool using graphical user interface or by CLI	Full fledged capability to configure the systems in a carrier grade manner
DNS Resolution	Rotate traffic incoming to multiple groups of AG1000 systems by providing resolved IP addresses to DNS queries from transaction terminals. Criteria selection decided on multiple criteria including run time identification by traffic volume, processing delays, overall speed, etc.	Designated AG1000 system can act as internal DNS server to intelligently distribute traffic across multiple AG.
Hardware Acceleration	The AG1000 hardware acceleration encryption engines to achieve the performance required for the financial market.	industry-leading performance on a small form factor.

NewNet
SECURE PAYMENT TRANSACTIONS

AccessGuard 1000 Key Features

SSL Offloading

The NewNet AccessGuard 1000 solution uses next generation hardware acceleration encryption engines to achieve the performance required for the financial market. This means that with AccessGuard 1000 SSL offloader, the host system is not responsible for processing any portion of the SSL traffic. By processing the entire SSL transaction, AccessGuard 1000 uses a model of encrypted-data-in from POS to decrypted-data-out towards the host system. AccessGuard 1000 system supports the various flavors of TLS including TLS v1.0, TLS v1.1, TLS v1.2.

SSL Acceleration

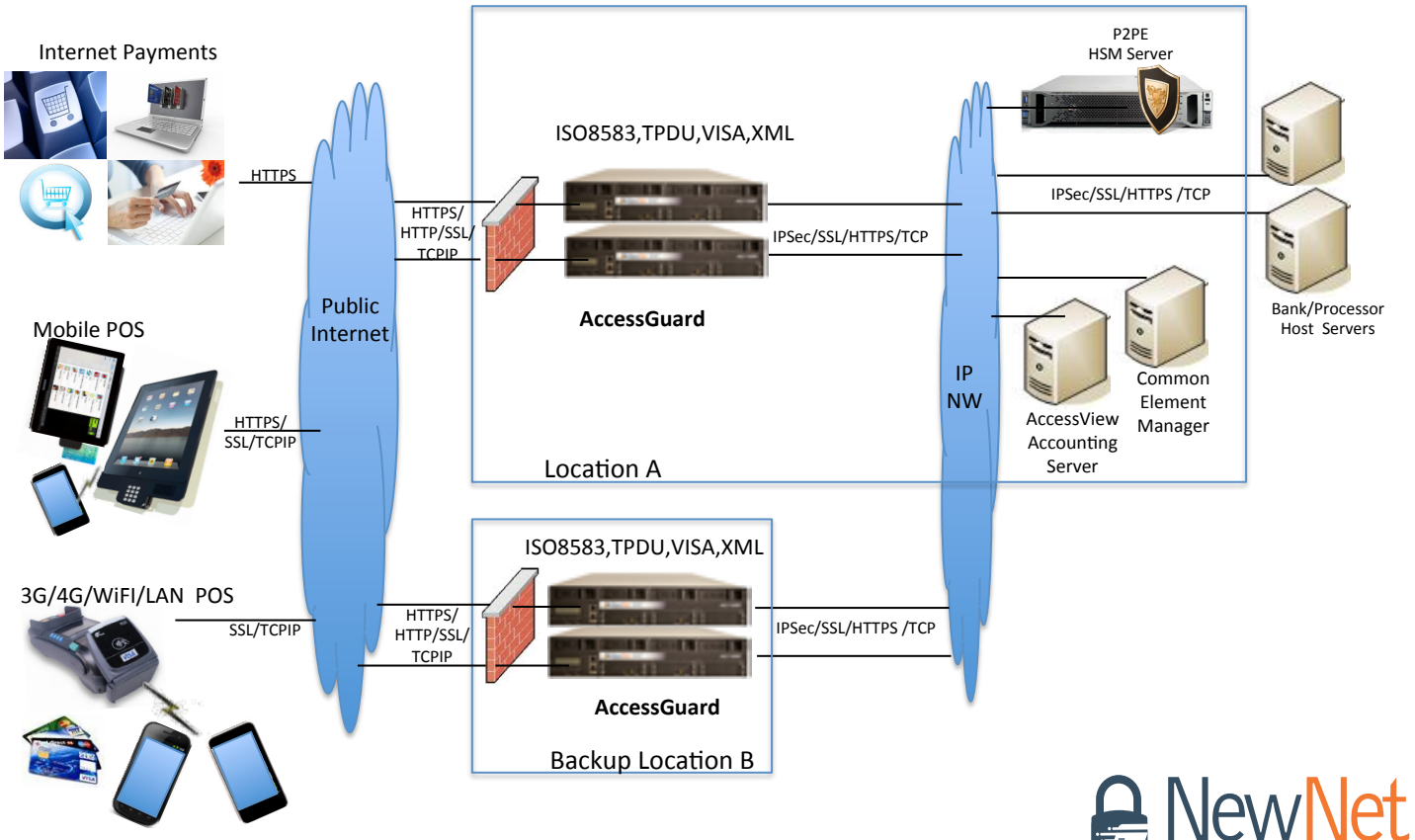
The NewNet AccessGuard 1000 solution can aggregate thousands of persistent and non-persistent SSL connections and transactions. AccessGuard 1000 can also support sessions re-use, introduced in TLS 1.x which is used to reduce the burden of establishing a new SSL session by reusing previously established SSL Session ID's.

HTTPS Transactions

AccessGuard 1000 enables the routing of HTTPS transactions (HTTP with SSL) which may encapsulate VISA/ ISO8583/TPDU/Custom messages and transporting these protocol data to Host servers. This integrated model allows the support of TCP/IP, SSL over TCP/IP and HTTPS transactions on a single AccessGuard 1000 system.

Redundancy & Load Sharing

The NewNet AccessGuard 1000 solution is designed to eliminate the single point of failure inherent in the IP environment. AccessGuard 1000 can support VRRP (RFC 3768), which provides dynamic fail-over in the forwarding responsibility, should one AccessGuard 1000 become unavailable. This provides a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every IP POS devices. AccessGuard 1000 can also be integrated with DNS server to support DNS round robin for load sharing.



NewNet
SECURE PAYMENT TRANSACTIONS

NewNet AccessGuard Advantages

Leverages Years of Experiene In Processing

The NewNet's Payment Transaction Processing Solutions have a customer presence across the globe, with service and support responsibilities for over 30 customers across 44 countries. TraxcomSecure payment routing and processing solutions process multi-billion transactions annually with major deployments at global acquirers, processors, carriers and banks. Many of these deployments across all geographies are countrywide implementations of the solution. The TraxcomSecure systems process about 20% of the global annual transaction volume, with 1 in 4 transactions in North America, 1 in 3 transactions in South America and 1 in 4 transactions in the Asia-Pacific regions.

Integreated with Accounting and Network Management Products

The AccessView Accounting Server, which is an integral part of Newnet's transaction processing suite or products, captures accounting and network statistics from the AccessGuard 1000 System. The data captured by the accounting server supports subscriber billing, transaction recording, report generation, network performance monitoring, and system modeling and measurements.

The Common Element Manager System (CEM) provides flexible, centralized management for the TraxcomSecure family of products. This powerful solution enables performance, fault, and configuration management of single and multiple AccessGuard chassis and their components in all NewNet based service environments.

Multi-Mode Rules Based Routing for Intelligent IP Payment Transaction Processing

AccessGuard 1000, PCI DSS compliant Secure IP Transaction switching and routing gateway enables carriers, acquirers, processors and service providers the opportunity to route electronic payment transactions originating from any POS or transaction initiating device to an any authorization server based on, but not limited to the following criteria:

1. Least Cost Network Route
2. Network availability
3. Shortest path
4. Server availability
5. Server Traffic
6. Pending transactions

Apart from a network specific destination, the AccessGurad 1000 system offers the option to route transactions in real time, to specific acquiring banks, processing host servers or other financial institutions based on the transaction fees charged by the various entities.

Depending on the fee charged by the acquiring institution, the AccessGuard 1000 will route the transaction to the lowest fee charging authorization server for a particular type of transaction. This includes varying fees for transactions like credit, debit, prepaid, mPayments, and PayPal.

The AccessGuard 1000 will intelligently select the lowest fee charging destination based on the type of the transaction and specific card association, issuing bank or institution. These selections may be updated securely and dynamically via a HTTPS, based on changes in the rates offered by these institutions and the system will dynamically route the transactions real-time to the new destinations.

In addition to the direct selection of the lowest fee based destination servers, other possible secure routing may be applied in combination, with specific rules like:

1. Preferred server for specific type of transactions
2. Selected server for transaction values above certain ranges
3. Specific server for transactions from select locations
4. Designated server for low value transactions
5. Higher fee server for high risk, low security area transactions

In today's dynamic, volatile and fiercely competitive settlement of payment card and third party network transactions markets, secure and timely flexibility of routing and processing options insure minimizing fees and maximizing network processing efficiencies.

Integrated Solution

The AccessGuard 1000 solution supports transaction processing, security off-loading and network routing in a single box. It can also be used with the currently deployed point-of-sale (POS) terminals.

Low Cost Ownership

AccessGuard 1000 is built for delivering high call density in 2U of rack space.

Highly Versatile System

Integrated processing of internet payment transactions, mobile POS transactions and NFC mobile wallet payments.

Scalability And Reliability

Designed to scale from supporting hundreds of mobile, broadband IP payment terminal support tens of thousands of terminals. The AccessGuard 1000 solution is designed to eliminate the single point of failure inherent in the IP environment.

Contact Us

traxcominfo@newnet.com
www.newnet.com