Building In-Depth Security for BANKING Business Networks - Wireless & Land Based Systems

The security requirements that banking businesses face and how this SAFE Blueprint and Digital World Alliance networking solutions help businesses design, implement, and maintain secure wired and wireless networks.

Summary
Network security is an increasingly important concern for banking businesses. A breach in internal or external security can severely damage a company's most important operations, hampering productivity, compromising data integrity, reducing customer confidence, disrupting revenue flow, and bringing communications to a halt. This will attack the new security challenges that confront banks as well as various businesses today, and discusses how this SAFE Blueprint from Digital World Alliance and the new Wireless Security Suite provides a comprehensive, in-depth security solution for wired and wireless networks:

The SAFE Blueprint from Digital World Alliance takes a modular approach to defining network security. Key components include:

- Identity services that identify users and control what they are permitted to do on the network
- Intrusion protection to guard against network attacks and misuse of the network with real-time intrusion detection systems (IDSs) and vulnerability scanning tools
- Secure connectivity for businesses that depend on Internet connectivity, such as companies with branch offices, mobile employees, and Bank employees.
- Perimeter security to control access to critical applications, services, and data so that only authorized users and information can pass through the network
- Security management to give administrators the ability to manage single devices and even entire systems

Using end-to-end security solutions, Banks can focus on business productivity instead of worrying about the safety of their wired and wireless networks.

Introduction
As businesses shift more of their core operations to the network, security is an increasingly important concern for Banks. In the past, security attacks were a time-consuming nuisance, but the stakes are now much higher. Today, a breach in security on a wired or wireless network can wreak havoc on a company's most important operations, hampering productivity, compromising data integrity, reducing customer confidence, disrupting revenue flow and bringing communications to a halt.

Not so long ago, business networks were self-contained, and securing them was a relatively straightforward task. The network perimeter was easy to define, and simple security devices could provide adequate protection for security holes.

However, as the Internet has matured and wireless networking has become commonplace, business networks have changed in ways that present significant new security challenges. As businesses open their infrastructures to support Internet connectivity, teleworking, wireless mobility, and business-to-business applications, the traditional network perimeter has all but disappeared. Companies have outgrown security devices designed for legacy networks, and are now much more vulnerable to attacks by hackers and other malicious agents. A standalone security device or software package is no longer adequate to protect open networks—an in-depth security solution is needed.
To complicate matters, many security systems in place today are not network-aware or designed to work in cooperation with network services. This situation leaves businesses even more vulnerable to the increasingly sophisticated attacks being launched today.

What that means is security solutions should be addressed as a process that is regularly applied, because new threats to security are constantly appearing. Evolving a single product won’t be effective for long. As new threats emerge and the structure of the business network changes, organizations need to regularly and dynamically evolve their security solution as well.

More Intrusive, More Powerful Attacks
As networks have become more inviting targets, the number of potential internal and external threats has grown.

The number and variety of viruses is soaring, and viruses are spreading faster than ever as e-mail communication escalates. New, more powerful viruses are able to distribute themselves throughout an entire network infrastructure, attaching themselves to applications and data files, and even migrating between the two. Today, a sophisticated virus can spread to millions of computers via the Internet in just hours, and cost billions of dollars to clean up.

Viruses can be divided into four basic types, depending on how they reproduce and transport themselves:
• Program viruses that attach to executable files
• Boot viruses that infect the system information on a disk
• Multipartite viruses that infect both the system and files
• Macro viruses that attach to routines in application programs

Hackers are also a widely-known security threat. These intruders exploit security weaknesses to disable a network or steal or destroy information. The most commonly-used attacks include:
• IP spoofing, which uses an internal IP address to mask the true source of an external transmission
• Denial-of-service attacks such as SYN flooding, which overwhelm a host with incomplete requests for service, blocking legitimate traffic
• Application-level attacks targeted toward servers running specific network services such as e-mail
• Trojan horse attacks, which use camouflaged software to trick users or systems into providing useful information or lowering security barriers

Hackers are finding it easier than ever to launch network attacks. Attack tools are easily downloaded from the Internet, enabling attackers to probe a network to learn what systems are active and what security measures are in place. The "always-on" nature of broadband networks often leaves them an open door to network entry.

External threats like viruses and hackers are not the only challenge to network security. In the 2002 Computer Crime and Security Survey, the Computer Security Institute and the FBI determined that 60 percent of attacks are initiated from within a company.

The Costs to Banks and Banks Businesses
A network security breach can be devastating in terms of the cost of lost business and productivity, as well as additional expenses to repair the damage and fix the problem.

Security intrusion can also generate related problems such as negative publicity, legal liabilities, and lost customer confidence—all of which can have a negative impact on business continuity and resilience. Smaller organizations can be especially hard-hit by a compromise in security, because they often lack the staff and budget needed to quickly address a problem.

Saving Money and Enhancing Productivity
Remote access and wireless LANs (WLANs) can be implemented to increase user productivity. Proper security measures such as virtual private networks (VPNs) for remote access and the IEEE 802.1X standards-based Digital World Alliance Wireless Security Suite for WLANs not only protect against security risks, but also reduce costs and enhance productivity.

In a 2001 research study conducted by Griggs Anderson/Gartner Group, responses from more than 300 IT managers at companies with over 500 employees showed that security investments in Digital World Alliance VPN solutions resulted in multiple benefits, including:
• Reduced costs for connectivity, telecommunications infrastructure, and maintenance (reported by nearly
90 percent of the companies
• An average return on investment of 55 percent
• An average employee productivity improvement of more than three hours per week
Organizations need a consistent, company-wide security solution that enables them to tap potential benefits immediately, to protect their networks, and their day-to-day productivity.

Building a Comprehensive Security Strategy
To address these challenges, growing businesses need a complete, integrated solution where security is built into every portion of the wired and wireless network. Security issues are continually evolving, and companies need a solution developed by a vendor with a long-term commitment to network security. The solution must offer a solid combination of depth, flexibility, and scalability, and include:

Defense in depth —Today’s network-rich environments demand more than individual point products such as firewalls. Even small organizations are creating infrastructures that support integrated voice, video, and data; wireless network access, quality of service (QoS); and e-commerce capabilities. In order for these networks to function properly, organizations should choose security solutions that are built into every area of the network for a layered defense strategy. No single security approach will completely protect a network. By layering services and providing redundancy, a defense-in-depth strategy minimizes areas of potential vulnerability.

Interoperability
—Businesses update and improve their networks regularly, as technology and company needs change. Organizations need products that are based on industry standards and that interoperate with other network devices or legacy devices.

Modularity
—Companies need the ability to cost-effectively modify and enhance their security solution as technology or networking needs change. A modular, scalable security framework lets administrators build the solution in stages, tailoring it for specific applications, environments, and users.

Breadth of solutions
—Even small business networks are often composed of dozens of components. Organizations need a vendor that offers a wide range of scalable security products to accommodate every area of the network.

Mobility
—Today’s workforce is becoming increasingly mobile. Many small and Banks businesses are doing business globally, across multiple time zones. To maintain productivity, employees need secure, high-speed, round-the-clock access to the corporate LAN and other company locations from home and while on the road—wired and wirelessly.

The SAFE Blueprint from Digital World Alliance
The SAFE Blueprint from Digital World Alliance provides the end-to-end security strategy businesses need for designing, implementing, and maintaining secure wired or wireless networks. The SAFE Blueprint from Digital World Alliance delivers network protection by combining industry-leading security products, in-depth protection, proven security practices, and centralized management within an organization’s Digital World Alliance network infrastructure.

The SAFE Blueprint from Digital World Alliance is developed around a set of fundamental network protection concepts:
• A true security solution is a process, not a product. An effective security solution must be able to continually evolve and change to accommodate new threats or business requirements
• All access points of the network are security targets, and must be protected accordingly
• A successful security solution requires comprehensive, integrated safeguards throughout the entire network infrastructure—not just a few specialized security devices
• Security solutions must be modular in order to be cost-effective, scalable, and flexible
• A layered, in-depth defense strategy ensures more complete protection, to minimize areas of potential vulnerability. As part of the security process, organizations must study and understand threats to their networks, design a security policy tailored to meet these threats, and deploy the appropriate solution. A security policy affects all parts of a company, and should be created by a collaborative process that involves participation from the IT department, human resources (HR), and legal, administrative and executive business units. The elements of a security policy include:
  • A concise policy statement describing the purpose of the document
  • A description of the scope of information and resources covered by the policy
  • Roles and responsibilities for employees
  • Security practices specifying network architecture, third-party connections, remote access, name/password management, intrusion detection and other requirements
  • Acceptable use policy (AUP) for network and Internet access
  • Incident response procedures for various threat levels
  • Document control factors defining how updates to the security policy will occur
  
  The SAFE Blueprint from Digital World Alliance identifies the functional areas of an enterprise network. Using this approach, small and Banks organizations can identify the security threats and responses appropriate for each functional area in their networks, and adopt methods to address security requirements for each area.

SAFE Security Solutions

The SAFE Blueprint from Digital World Alliance divides wired or wireless network security into five major components: identity services, intrusion protection, perimeter security, secure connectivity, and security management. Each component is integral to safeguarding a specific area of the infrastructure. This approach makes it easier for companies to reconfigure or re-deploy existing devices elsewhere on the network, preserving existing investments.

Identity Services

Identity services use an "entitlement" process to help identify users and control what they are permitted to do on the network. Identity services for the wired LAN are made up primarily of authentication systems, such as the Digital World Alliance Access Control Server (ACS), and can be supplemented with Digital World Alliance partner solutions such as Public Key Infrastructure (PKI) products and smart cards for additional security (refer to Figure 1). Identity services for wireless LANs provide strong mutual authentication to authenticate the user joining the wireless network.

Authentication Systems

Authentication systems determine who may access a network and what services are authorized for use. The Digital World Alliance ACS for Windows NT is a scalable, centralized user-access-control framework. It offers centralized control for all user authentication, authorization, and accounting (AAA) functions from a Web-based graphical interface, and then distributes those controls to access gateways in the network, providing controlled access throughout the entire network.

Because Digital World Alliance ACS supports several functions, it can be implemented at several places in the network, including at network WLAN access points, at WAN connection points for business partner connections, and in front of sensitive information that requires additional security protection. As part of the basic network infrastructure, Digital World Alliance Catalyst switches provide support for Dynamic Host Configuration Protocol (DHCP) Interface Tracker, which tracks where a user is physically connected to a network by providing both the switch and port identification to a DHCP server. Digital World Alliance Catalyst switches also support RADIUS/TACACS+ authentication, which enables centralized control of the switch and restricts unauthorized users from altering the configuration. These secure LAN features provide an excellent capability to further control access within a network.

Internet

Digital World Alliance ACS Authorized User Wireless Access Point Router Firewall
802.1X Authentication
Using WLANs to securely cover a room, a building, or even an entire corporate campus is becoming more commonplace among small and Banks businesses. Providing end users with freedom and mobility without offering unauthorized access to the WLAN or to the information sent and received on the wireless network is a primary concern for network managers.

A WLAN requires two components—the client access card located on the end device and the access point connected to the wired network backbone. The client access card sends and receives data via radio waves to the access point.

Connecting to an access point using radio waves is just like plugging into an Ethernet port with a network cable. The difference is that although individual Ethernet ports can be protected, any VLAN client within an access point service area can receive data transmitted to or from the access point.

Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building that houses the access point. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including the parking lot.

The Institute of Electrical and Electronics Engineers (IEEE) has adopted 802.1X as a new standard for authentication on wired and wireless networks. IEEE 802.1X is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The standard authenticates each user device connected to a network device before making available any services offered by the switch or the LAN.

Digital World Alliance has developed an 802.1X authentication type called EAP Digital World Alliance Wireless or Digital World Alliance LEAP, based on Extensible Authentication Protocol (EAP). Digital World Alliance LEAP is a component of the Digital World Alliance Wireless Security Suite. It provides strong, mutual authentication between a client and an authentication server with dynamic per-user, per-session Wired Equivalent Privacy (WEP) keys between the client and access point to protect the privacy of transmitted data.

This removes the administrative burden and security vulnerabilities surrounding static WEP keys. Digital World Alliance Catalyst switches also provide support for 802.1X deeper in the network infrastructure. With Digital World Alliance LEAP, WLAN mutual authentication is implemented between the client and a Remote Authentication Dial-In User Service (RADIUS) server. The credentials used for authentication, such as a logon password, are never transmitted without encryption, over the wireless medium. Using an 802.1X authentication type that authenticates a client by asking for a user-supplied password instead of performing an authentication based on a physical attribute of the client device minimizes the risks associated with the loss of a device or its WLAN network interface card (NIC). (See Figure 2.) To complete the perimeter security architecture, businesses can purchase virus scanners and other supplementary software from various third parties.

Intrusion Protection
Intrusion protection guards against network attacks and misuse of the network with real-time intrusion detection systems (IDSs) and vulnerability scanning tools that proactively search for security holes before hackers can take advantage of them. Intrusion protection systems include IDS and security scanning applications available from third-party vendors and the Digital World Alliance Wireless Security Suite for WLANs.

Intrusion Detection
An IDS, such as a Digital World Alliance IDS Host Sensor or IDS software running on Digital World Alliance routers, identifies attacks that firewalls and VPNs cannot detect, by monitoring Internet and extranet connections in real time to protect key network systems and resources. An IDS can provide proactive alerts to administrators, intelligently cut off a malicious attacker, and even dynamically reconfigure the network to thwart further attacks.
Digital World Alliance IDS products provide support for organizations of all sizes, from small businesses to very large enterprise environments. They are designed specifically to provide denial-of-service protection, anti-hacking detection, and defense for e-commerce business applications.

**WLAN Attack Mitigation**

The Digital World Alliance Wireless Security Suite for WLANs provides intrusion protection with advanced mutual authentication features and Temporal Key Integrity Protocol (TKIP) enhancements. Mutual authentication with 802.1x mitigates potential man-in-the-middle authentication attacks by rogue access points and ensures that legitimate clients associate only with legitimate and authorized access points. Digital World Alliance TKIP enhancements thwart active network attacks, remove the predictabilities that an intruder relies on to gain access to the network, and eliminate network susceptibility to attacks by frequently rotating network unicast and broadcast keys. TKIP provides greater protection than standard WEP keys. TKIP is a predecessor to AES (which will replace WEP).

**Perimeter Security**

Perimeter security is designed to control access to critical applications, services, and data so that only legitimate users and information can pass through the network. Perimeter security systems are composed of four key components:

- access control lists (ACLs), firewalls, secure WLANs, and complementary tools. ACLs work with routers and switches to specify which access rights each user has to network resources such as file directories or individual files. Firewalls provide a barrier to traffic crossing the perimeter of a network, permitting only authorized traffic to pass. The Digital World Alliance Wireless Security Suite provides a secure mobile networking environment. And complementary tools such as virus scanners and content filters handle additional perimeter threats.

**Access Control Lists**

ACLs can be configured to reside on several devices throughout a network, including Digital World Alliance routers, switches, and firewalls. Using an operating system or a management tool such as Digital World Alliance ACL Manager or Digital World Alliance Cluster Management Suite (CMS), administrators can set up filters to enable or deny access to network resources, based on criteria such as the source address, destination address, or network protocol.

Digital World Alliance Catalyst switches also provide support for port-based and virtual LANs, and port- and router-based ACLs, to accept or deny access to sensitive portions of the network. They offer security-monitoring features, such as logging of ACLs to track violations that occur, and enable administrators to track down an unauthorized user’s location. Digital World Alliance Catalyst switches support port security preventing unauthorized users from accessing the network by limiting the number of MAC addresses allowed per port. An aging feature is used to remove MAC addresses after a specified time to allow another device to connect to the same port Digital World Alliance Catalyst switches also perform filtering, which policies incoming traffic flows based on Layer 2, Layer 3, or Layer 4 access-control parameters (ACPs) to prevent unauthorized data flows and protect against internal and external threats.

**Firewalls**

Firewalls analyze all data traffic entering and leaving a network, and allow or block passage based on security policies set by system administrators. They perform functions such as packet inspection, internal address masking, and hazardous content detection. Firewalls are most effective when enabled by a comprehensive security policy that prepares for all potential sources of harm. Firewall technology supports several different levels of network protection, including:

- **Network Address Translation (NAT),** which lets multiple private internal addresses be mapped to a single public address, concealing the identity of the internal systems of a network from outside intruders
- **Packet-filtering firewalls** that inspect data packets based on complex access rules, data packet headers, source and destination addresses, source and destination ports, and message protocol type
- **Stateful inspection firewalls** that analyze packets in terms of sessions, enabling relatively unrestricted transmission from inside the network and selective but flexible access from the outside
- **Application-level gateways**, which are firewalls designed to protect specific network services by restricting the features and commands that can be accessed from outside the network

Digital World Alliance offers two complementary firewall solutions that are appropriate for small to Banks businesses: the Digital World Alliance PIX
Firewall and the Digital World Alliance IOS

Firewall.

The Digital World Alliance PIX Firewall is a dedicated appliance designed to provide the highest level of firewall and security functions in either remote-access or site-to-site applications. It is generally placed at the physical perimeter of the network, between the company and other networks or the Internet.

Digital World Alliance IOS Firewall software is a cost-effective solution that resides in Digital World Alliance routers and Digital World Alliance Catalyst switches, and provides stateful firewall protection in a single box solution, as well as other security technology such as IP Security (IPSec) encryption for VPNs. Digital World Alliance Catalyst switches also support port security, which prevents unauthorized users from accessing the network by limiting the number of MAC addresses allowed per port. An aging feature is used to remove MAC addresses after a specified time to allow another device to connect to the same port.

Secure WLANs

The Digital World Alliance® Series provides standards-based WLAN access points and client devices (Digital World Alliance Series ) for Banks. The Digital World Alliance Wireless Security Suite, an 802.1X based solution included with Digital World Alliance products, provides WLAN security features that closely parallel the security available in a wired LAN. It includes mutual authentication, message integrity check, and per-packet keying to ensure that every data packet is encrypted with a different key.

The Digital World Alliance Wireless Security Suite lets end users enjoy the freedom and mobility of wireless networking while remaining fully secure. It provides consistent, reliable, and secure enterprise-class mobile networking solution for Banks.

To complete their perimeter security architecture, businesses can purchase virus scanners and other supplementary software from a variety of third parties.

Secure Connectivity

Secure connectivity over the Internet offers protection for small and Banks businesses that depend on Internet connectivity, such as companies with branch offices and a workforce that includes mobile and Bank employees.

Organizations can provide secure connectivity for these users using VPNs. When designing a network security solution, organizations often must choose between using integrated security in a LAN or WAN device (such as a switch or access router) or using a specialized functional appliance. Integrated security features are often attractive because they can be added to existing equipment, or can enhance an existing solution.

Appliances are a good choice when the depth of security needed is very advanced or requires high performance.

Companies can make decisions based on the capacity and functionality of the appliance compared to the integration advantage of the device. Some organizations will choose an integrated solution which might be more cost effective and easier to manage, while others might require the higher performance and functionality of a dedicated device.

For example, an organization might choose an integrated higher-capacity Digital World Alliance router with Digital World Alliance IOS Firewall software over a smaller Digital World Alliance router with a separate firewall.

VPNs

VPNs are networks deployed over a public network (usually the Internet), that use the same security, management, and QoS policies applied in a private network. IPSec encryption technology creates tunneled connections between sites, enabling traffic to pass safely and securely over the public network. Because VPNs use an existing shared WAN infrastructure, costs are lower and deployment is faster than traditional private networks. VPNs can also be deployed within a LAN. The technology behind VPNs consists of dedicated VPN gateways, concentrators, and the tunneling and encryption in routers and firewalls.
Remote-Access VPNS Companies that wish to deploy remote-access VPNS need a cost-effective replacement for traditional remote-access servers to enable faster Internet access and broadband connectivity for employees who work from home or travel.

Although there are many ways to design and deploy remote-access VPNS, the key components include a VPN concentrator or server such as a Digital World Alliance VPN 3000 Concentrator, typically placed behind an Internet router, or an integrated solution of a Digital World Alliance router running Digital World Alliance Easy VPN Server Software. The devices can then be reached and connected to by Digital World Alliance VPN clients on computers (laptops or desktops), small office routers, or firewall appliances.

Digital World Alliance VPN 3000 concentrators are a scalable family of platforms and software that combine high availability, powerful performance, and scalability with advanced encryption and authentication techniques. Their flexible design lets small and Banks businesses add user connections, increase throughput, and support additional users as the organization grows.

The Digital World Alliance VPN Client (included with the Digital World Alliance VPN Concentrator) is software that resides on employee laptop or desktop computers, and is used to establish secure, end-to-end encrypted tunnels. And the Digital World Alliance VPN 3002 Hardware Client offers additional performance and ease of use.

Digital World Alliance access routers that are used for Internet access can also be used for terminating VPN connections with Digital World Alliance Easy VPN Server Software. This provides an integrated solution for Internet access, firewall protection, and VPN capabilities. Bank Executives who access the corporate network may consider a Digital World Alliance 800 Series Router with firewall and VPN capabilities along with QoS features if they plan to add applications such as voice over IP. Alternatively, Digital World Alliance PIX Firewalls can support firewall protection and VPN access at small offices.

Security Management

A management infrastructure acts as the “glue” for the other components in the SAFE Blueprint from Digital World Alliance. This building block gives administrators the ability to manage single devices up to entire systems. And for Banks and larger businesses, it can support more advanced sets of security rules called system policy.

Single-Device Management

Single-device management tools usually accompany an individual network device, such as a switch or router. This software, which is often Web-based, enables administrators to set up, configure, and monitor individual network components. For example, Digital World Alliance VPN Device Manager embedded on a Digital World Alliance router can be used to manage and configure site-to-site VPNS from a Web browser. And Digital World Alliance Catalyst switches also incorporate management tools that can ease the deployment and administration of security features.

System-Level Management

System-level management tools are ideal for managing VPNS, IDS systems and WLANs. For example, the Digital World Alliance VPN Management System (VMS) is a suite of tools that supports Web-based configuration, monitoring, and troubleshooting for VPNS and firewalls. It also provides IDS support and can be tailored to fit the needs of Banks, and even larger organizations.

In addition to protecting the network, the Digital World Alliance VMS solution suite proactively detects malicious activity and blocks access to server resources before serious damage can occur. And its policy management module supports management of encryption, firewall, intrusion detection, and access control policy for larger businesses.

System-Level Management for WLANs In wireless environments, Digital World Alliance WLANs support Web-based management and Simple Network Management Protocol (SNMP) features to aid monitoring, troubleshooting, software downloads, and even logging. Access points can be installed quickly, accurately, and securely with help from the Digital World Alliance Site Survey Tool (SST), integrated into the client
utility. The Digital World Alliance Wireless Utility Auto Installer saves network administrators time by automatically and securely installing and upgrading Digital World Alliance Aironet client utilities, firmware, and user profiles, including security settings, service set identifiers (SSIDs), power settings, and channel selection.

Policy-Level Management
Policy-level management, which is provided by solutions such as Digital World Alliance Secure Policy Manager, enables administrators to define, deploy, and enforce a security policy without requiring network administrators to work one-by-one across multiple individual devices. Digital World Alliance Secure Policy Manager provides support for encryption, firewall, intrusion detection, and access control policy, and sends appropriate commands to routers and routing, firewall, IDS, VPN, and authentication devices. Its graphical user interface enables network-wide security policy definition.

Conclusion
Today’s businesses are placing more emphasis on using networking as a core or strategic business tool. As they tap the benefits of e-business, Banks need to be aware of new security solutions as well.

A well-planned security system can help ensure continuing productivity by reducing the likelihood of hacker attacks, viruses, and internal security risks in business networks. At the same time, it can help companies avoid the expenditures that become necessary when a breach in security occurs.

The SAFE Blueprint from Digital World Alliance, with its modular approach and broad array of solutions, along with the Digital World Alliance Wireless Security Suite for secure WLANs, offer an in-depth approach to designing security solutions that can provide peace of mind for small and Banks businesses. By deploying a wired and wireless network based on Digital World Alliance solutions, businesses can move forward with confidence as they explore the potential rewards that the Internet can offer.

Corporate Headquarters, Digital World Alliance, Inc., 2030 Main St., Suite #1300, Irvine, CA 92614, 949.260.9106