

Banking Regulators Emphasize Need for Self-Defending Network

Table of Contents

What is a SDN?	1
Overview of FFIEC Criteria for:	
- Adaptive Security Appliance	1
- Cisco Security Agent	2
- Network Application Control	2
- Cisco Security-MARS	3
Where can you learn more?	4

Attachment A - FFIEC SDN Chart

SIMPLER  WEB B

This paper reviews the
the self-defending network
criteria mandated in the
FFIEC IT guidelines.

May 2007

Effective July 2006, the Federal Financial Institution Examination Council (FFIEC) updated the Gramm-Leach-Bliley (GLBA) Information Security standards¹. These new mandates emphasize the need for each financial institution to adopt a proactive self-defending network (SDN) capability as part of its information security program.

In this paper, we provide information on the general framework and definition for a SDN, review the specific criteria in the FFIEC booklet that mandate a SDN framework, and identify specific Cisco solutions that create a proactive SDN and can enable compliance.

WHAT IS A SELF-DEFENDING NETWORK?

The banking regulators now require financial institutions to evolve beyond point-security products to an integrated security strategy that establishes perimeter security as well as security inside the network and among all end-point devices, e.g., laptops, PCs, wired and wireless devices, PDAs, and more. All devices on the network must:

- Collaborate to ensure proactive security is working effectively.
- Adapt in real-time to the institution's changing risk profile and new security threat events as they occur.

Financial institutions cannot achieve this proactive security culture without the help of automated security solutions that are integrated throughout the network to enable real-time monitoring of all network activity. They must have a centralized security monitoring capability that will allow them to prevent, detect, and respond rapidly in real-time.

“A self-defending network provides institutions with the ability of the network to protect, detect, and respond to threats. It provides an automated systems approach to stop the bad stuff - only the bad stuff - from entering the network.”

The Cisco Self-Defending Network solution enables financial institutions to comply with the FFIEC information security mandates. The primary components of the Cisco SDN that enable this compliance are the: Adaptive Security Appliance (ASA); Cisco Security Agent (CSA); Network Admission Control (NAC) appliance; and Cisco Security Monitoring, Analysis, and Response System (MARS). Each of these SDN components is described below in greater detail and further aligned to the specific FFIEC mandates that it helps enable in the attached chart that follows.

WHAT IS THE ADAPTIVE SECURITY APPLIANCE (ASA)?

Firewalls are essential. However, today's firewalls must be able to adapt and prevent spam, viruses, and spyware, and filter web content in real-time. The FFIEC emphasizes the need for a strong intrusion detection and prevention capability throughout the network, not just at the perimeter anymore.

“Networks provide system access and connectivity between business units, affiliates, partners, customers, and the public. This increased connectivity requires additional controls to segregate and restrict access between groups and users. An effective approach to securing a large network involves dividing the network into logical security domains. A logical security domain is a distinct part of a network with security policies that differ

¹ A copy of the FFIEC Information Security Handbook is available at www.ffiec.gov/ffiecinfobase/index.html.

from other domains, and perimeter controls enforcing access at a network level. The differences may be far broader than network controls, encompassing personnel, host and other issues.

- July 2006 FFIEC IT Information Security Examination Booklet, P. 38.

Cisco's Adaptive Security Appliance (ASA) is the next generation of the PIX firewall that provides these capabilities. It protects the perimeter and moves the intrusion detection capabilities into the network to provide converged firewall, intrusion prevention systems, and network anti-virus and VPN services. ASA allows you to filter and monitor network traffic across multiple security domains and stops attacks before they spread through the network.

WHAT IS THE CISCO SECURITY AGENT (CSA)?

Zero-day exploits – which take advantage of security vulnerabilities as soon as they are discovered, before vendors can patch their products – create a significant network security threat. Because of these and other sophisticated emerging threats, the regulators have enhanced the information security strategy, controls, and monitoring guidelines. For example, they have added criteria for institutions to deploy prevention, detection, and response mechanisms. Additional focus is also placed on the importance of limiting access to the network and sensitive data to a “need-to-know” basis. This requires institutions to implement least permissions and least privilege policies for network access.

“Prevention addresses the likelihood of harm. Detection and response are generally used to limit damage once a security breach has occurred. Weaknesses in prevention may be offset by strengths in detection and response...Security strategies should establish limitations on access and limitations on the ability to perform unauthorized actions. Those limitations derive from concepts known as security domains, least permissions, and least privileges.”

- July 2006 FFIEC IT Information Security Examination Booklet, P. 18.

Cisco's ASA analyzes behavior on the network to create a proactive – not reactive – security capability. In addition, the Cisco Security Agent goes beyond signature matching for known threat events and analyzes behavior patterns for known, new, and unknown threat events. This dynamic behavior-analysis capability allows CSA to help prevent, identify, and eliminate attacks from emerging threats. For example, CSA and ASA collectively offer several security functions (e.g., host intrusion prevention, distributed firewalls, anti-spyware/adware, malicious code filtering, and more) to proactively prevent zero-day attacks. Zero-day attack means that none of the security vendor products had an update to detect, prevent, or respond to the attack – it was an unknown threat. CSA also provides centralized security management capabilities. For example, you can use CSA to lock down administration rights to a specific personal computer or block USB ports and CD-Rom drives for helping to enforce a limited privileges policy and prevent data theft.

WHAT IS THE NETWORK ADMISSION CONTROL (NAC) APPLIANCE?

Each financial institution should have a control policy to monitor for patch updates and deploy such updates, as needed. No device should be allowed on the network that does not meet the criteria defined in this network admission policy.

The FFIEC now evaluates each institution's ability to enforce a control policy for vulnerability patch management and prevention of malicious code such as viruses, worms, and spyware from entering its network. They want to ensure that only authorized users are allowed on the network. In addition, each

user that is allowed on the network should comply with the institution's patch management and malicious code prevention policy.

“The goal of access control is to allow access to authorized individuals and devices and to disallow access to all others...Access should be authorized and provided only to individuals whose identity is established...Authorized devices are those whose placement on the network is approved in accordance with institution policy.”

- July 2006 FFIEC IT Information Security Examination Booklet, P. 22.

Cisco's Network Admission Control (NAC) appliance helps to enable compliance with this requirement. NAC evaluates each user device as it attempts to enter the network. It determines if the device is authorized to enter the network and if so, whether it is clean from malicious code and carries all of the necessary patch updates. If the device fails any of these tests, it can be quarantined until it meets all of the necessary criteria – helping to enforce policy compliance.

WHAT IS THE CISCO SECURITY MONITORING, ANALYSIS, AND RESPONSE SYSTEM (MARS)?

Cisco's Monitoring, Analysis, and Response System (MARS) provides a comprehensive monitoring and reporting capability to enable institutions to know, respond, and report on network activity. MARS gathers data from all devices on the network. With this data it can recognize and correlate real network attacks, define how to stop attacks, reduce false positives and allow resources to be more effectively focused on responding to material events, and simplify compliance reporting.

MARS allows institutions to log all security events, automate and streamline the log review process, notify and escalate material events to appropriate individuals, and retain evidence for forensic, audit, or examination review.

“Log files are critical to the successful investigation and prosecution of security incidents...Maintain a security response center that receives and analyzes the data flows as activity occurs...Security response centers (or personnel) should have available tools to analyze the logs and to perform ad hoc activity monitoring...”

- July 2006 FFIEC IT Information Security Examination Booklet, P. 87, 90, & 91.

WHERE CAN YOU LEARN MORE?

Additional information on the specific updates to the FFIEC Information Security guidelines is outlined in the attached chart with a reference to the applicable Cisco SDN solutions that help enable compliance with the guidelines. If you would like to learn more about the FFEIC mandates or solutions that can help you to create a competitive business advantage and comply with today's regulatory mandates, contact Simpler-Webb and the ReymannGroup to talk with one of our industry subject-matter experts.

ReymannGroup, Inc.

1908 Blue Ridge Road
Edgewater, MD 21037
USA

Phone: (410) 956 7334
Fax: (410) 956 7338
Email: info@reymanngroup.com

ReymannGroup, Inc. provides finance, healthcare, retail and manufacturing, and local and state government subject matter expertise. Our firm helps companies evaluate their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly-qualified professionals, authors of regulations and books, and subject matter experts familiar with industry regulations and best practices.

Simpler-Webb, Inc.

1717 West 6th St. Suite 140
Austin, TX 78703
USA

Phone: (512) 322 0071
Email: chris.cooper@swinc.com

Serving financial institutions since 1993, Simpler-Webb, Inc. provides a suite of managed services and technology consulting. Our products Managed Security, Managed Server, and Managed IT Infrastructure provide 24/7 support that allows credit unions and other financial institutions to focus on key business goals. Additionally, Simpler-Webb offers certified, experienced IT consulting for a variety of solutions including network optimization, wireless implementation, server virtualization, unified communications, and desktop/application assistance. As a Cisco Premier and Microsoft Gold Partner, Simpler-Webb delivers customized technology solutions that enable credit unions to compete successfully. We pride ourselves on the reputation we've earned as an extremely knowledgeable, cost effective, reliable and results-oriented technology partner. With Simpler-Webb, clients gain comfort in the knowledge that they are able to focus on vital business goals while our team of experts manages their IT operations every hour of every day.

WHAT ARE THE FFIEC SDN MANDATES?

The following chart highlights the FFIEC updates to the GLBA Data Protection rules and the components of the Cisco SDN that enable stronger network security and compliance with these mandates.

FFIEC SDN Mandate	CSA	NAC	ASA	MARS				
<p>I. SECURITY PROCESS</p> <p>Minimum Board Reporting The Board must now approve the information security program annually, not just once. There are now six specific examples of information that should be reported to the board. Four of these are focused on network security:</p> <ol style="list-style-type: none"> 1. Risk management and control decisions 2. Results of security monitoring and testing 3. Security breaches or violations and management’s responses 4. Recommendations for changes to the information security program <p><i>MARS provides the necessary real-time security monitoring and board reporting capabilities.</i></p>								
<p>II. INFORMATION SECURITY RISK ASSESSMENT – CRITERIA IS NOW CLEARER!</p> <p>The risk assessment market has matured with different types of methodologies. An FFIEC working group developed risk assessment guidance for the GLBA. That guidance has been incorporated into the Information Security Booklet. Specifically, the FFIEC now requires institutions to:</p> <ul style="list-style-type: none"> • Implement a strong security program to help reduce levels of reputation, operational, legal, and strategic risk. • Assess risk to all data, not just customer data. Therefore, financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories. <p>The FFIEC also updated the definition of an Information Security Risk Assessment. It now includes the need to “assess” threats – A process to identify and assess threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.</p> <p><i>SDN - The combined capabilities of CSA, NAC, ASA, and MARS allows the institution to identify and assess threats in real-time across the network.</i></p>								
<p>Gather Information More detailed examples of what to collect for an effective risk assessment are now defined. Examples include network maps detailing internal and external connectivity, hardware and software inventories, interfaces with external entities, and hardware and software configurations.</p> <p>Identify Information and Information Systems Information and information systems can be both paper-based and electronic-based. Include electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Include a system characterization and data flow analysis of networks (where feasible), computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems.</p>								

Attachment A

FFIEC SDN Mandate	CSA	NAC	ASA	MAR
--------------------------	-----	-----	-----	-----

II. INFORMATION SECURITY RISK ASSESSMENT – CONTINUED

<p>Have an Architecture Diagram The institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place.</p> <p><i>MARS provides a graphical view of all devices on the network. The information provided by MARS simplifies the data gathering and identification process.</i></p>				
<p>Consider Security on All Devices Consider backup tapes, portable computers, personal digital assistants, media such as compact disks, micro drives, and diskettes, and media used in software development and testing.</p> <p><i>NAC supports this risk assessment mandate by only allowing authorized and policy compliant user devices on the network.</i></p>				

III. INFORMATION SECURITY STRATEGY

FFIEC added more detailed guidance on the strategy for including:

<ul style="list-style-type: none"> Appropriate consideration of prevention, detection, and response mechanisms. <p><i>ASA & MARS -This is what the Cisco SDN does with the intrusion prevention capability delivered with ASA and the response and reporting capabilities in MARS.</i></p>				
<ul style="list-style-type: none"> Implementation of the least permissions and least privileges concepts. Policies that guide officers and employees in implementing the security program. <p><i>CSA centralizes enforcement of the least privileges and permissions. It enforces policy compliance for Internet use, USB storage devices, spyware and malware, and more. NAC provides an end-to-end network authentication, authorization, evaluation, and remediation of users and user devices before allowing them into the network.</i></p>				
<ul style="list-style-type: none"> Layered controls that establish multiple control points between threats and organization assets. Perimeter security is not enough by itself. Institutions need a security system that monitors across all devices and applications. <p><i>SDN – The SDN provides end-to-end layers of security across the network.</i></p>				
<p>Technology Design – Emphasizes Security Domains FFIEC describes the importance of security domains in accomplishing an appropriate technology design. They now also mandate that outsourced security services must be managed as if those services were performed in-house. You must design your technology to provide:</p>				
<ul style="list-style-type: none"> Effective network-level monitoring. <p><i>MARS ties into all network devices, IPS, and firewalls to give you network level system wide monitoring.</i></p>				
<ul style="list-style-type: none"> Limit an intruder’s ability to traverse the network. <p><i>ASA is an intrusion prevention system that provides proactive threat defense that stops attacks before they spread through the network.</i></p>				

FFIEC SDN Mandate	CSA	NAC	ASA	MAR
-------------------	-----	-----	-----	-----

III. INFORMATION SECURITY STRATEGY - CONTINUED

<ul style="list-style-type: none"> Update in a timely manner to mitigate newly discovered vulnerabilities. <p><i>ASA provides system updates to zero-day threats and NAC enforces updates for correct patches and signatures. Cisco's ASA allows you to filter and monitor traffic across multiple security domains.</i></p>				
<ul style="list-style-type: none"> Offer the minimum level of services required for business needs. <p><i>CSA centralizes enforcement of the least privileges and permissions. It enforces policy compliance for Internet use, USB storage devices, spyware and malware, and more. NAC provides an end-to-end network authentication, authorization, evaluation, and remediation of users and user devices before allowing them into the network.</i></p>				

IV. SECURITY CONTROLS

FFIEC has expanded its focus on external and internal security controls to respond to the increasing number of security events that are occurring.

<p><u>Access Control</u></p> <p>A new section on access controls was added that discusses the need for:</p> <ul style="list-style-type: none"> Controls over authorized devices in addition to authorized individuals. Access should be limited to known individuals and his or her activities should be limited to the minimum required for business purposes. Authorized devices on the network should be approved in accordance with a board approved policy. A risk assessment of Internet banking to determine the need for single versus multi-factor authentication. Stronger shared secret systems to help control keylogger and other monitoring device attack methods. Reissuing Authenticators. Behavioral-, device-, and mutual-authentication techniques. Offsetting controls to mitigate common threats such as warehouse attacks, social engineering, client attacks, replay attacks, man-in-the-middle attacks, and hijacking an authenticated user session. <p><i>CSA centralizes enforcement of the least privileges and permissions. It enforces policy compliance for Internet use, USB storage devices, spyware and malware, and more. NAC provides an end-to-end network authentication, authorization, evaluation, and remediation of users and user devices before allowing them into the network.</i></p> <p><i>ASA is an intrusion prevention system that provides proactive threat defense that stops attacks before they spread through the network.</i></p>				
<p><u>Network Access</u></p> <p>New guidance was added to expanding the examples of layered controls that help to prevent and detect unauthorized network access. The new controls that were added include:</p> <ul style="list-style-type: none"> Monitor cross-domain access for security policy violations and anomalous activity Malicious Code Filtering Outbound Filtering Network IPS (nIPS) Quarantining Devices DNS Placement Wireless Controls – Associated with network access 				

FFIEC SDN Mandate	CSA	NAC	ASA	MAR
-------------------	-----	-----	-----	-----

IV. SECURITY CONTROLS - CONTINUED

<p><i>SDN - The combined capabilities of CSA, NAC, ASA, and MARS allow the institution to establish the necessary layers of controls to identify and assess threats in real-time across the network. For example: CSA and ASA can protect against malicious code at the perimeter, cross domains, and at server and PC endpoints; NAC helps to ensure that your patches and policies are updated and working. It enforces security policies and quarantines devices that do not comply with the policy; ASA provides the necessary network intrusion prevention controls; and MARS provides a centralized capability to monitor devices, security policy violations, anomalous activity, and much more.</i></p>				
<p>Operating System and Application Access The FFIEC reiterated the need for adequate operation system and application access security. This guidance has not changed. It continues to provide a strong focus on restricting access, logging, and monitoring.</p> <p><i>CSA restricts access and MARS collects log information from all network devices to create a centralized view of all events and log data.</i></p>				
<p>Remote Access This section was updated to:</p> <ul style="list-style-type: none"> • Include extensive discussion of remote access over other than dial-up connections. • Require management approval for remote access. <p>For example, it now has an expanded list of remote access controls that should be considered such as encryption for a VPN, malware prevention, and much more.</p> <p><i>SDN - The combined capabilities of CSA, NAC, ASA, and MARS allow the institution to establish the necessary controls for remote access. For example: CSA and NAC work together to help prevent malware. NAC also enforces patch management for remote users; ASA filters traffic to help prevent intrusions that may originate from remote access; and MARS provides reporting capabilities to monitor and report on all access in and out of the institution.</i></p>				
<p>Encryption The FFIEC reiterated the need for employing encryption to protect sensitive data in storage and transit. The encryption guidance has not changed.</p> <p>Malicious Code Prevention The FFIEC revised its discussion of controls to protect against malicious code. It now provides additional guidance and examples on the need for host-, network-, and user-level controls to prevent and detect malicious code.</p> <p><i>CSA provides the host hardening and host IPS with anti-virus, -spyware, and rootkit. ASA enables IPS monitoring for inbound and outbound traffic. ASA also enables the transfer of encrypted data over a virtual private network (VPN).</i></p>				
<p>Systems Development, Acquisition, and Maintenance Updated with more specific guidelines to:</p> <ul style="list-style-type: none"> • Ensure that systems are developed and implemented with appropriate security features enabled. • Ensure that software is trustworthy by implementing appropriate controls in the development process, reviewing source code, reviewing the history and reputation of vendors and third party developers, and implementing appropriate controls outside of the software to mitigate the unacceptable risks from any deficiencies. 				

FFIEC SDN Mandate	CSA	NAC	ASA	MAR
-------------------	-----	-----	-----	-----

IV. SECURITY CONTROLS - CONTINUED

<p>Systems Development, Acquisition, and Maintenance - Continued</p> <ul style="list-style-type: none"> • Maintain appropriately robust configuration management and change control processes. • Establish an effective patch process. <p><i>SDN - The combined capabilities of CSA, NAC, ASA, and MARS allows the institution to establish the necessary technology infrastructure that allows systems to be developed, acquired, and maintained with appropriate security controls. For example: CSA delivers the hardening of the systems on the network; NAC enforces patch management; and MARS provides logging of network activity.</i></p>				
<p>Data Security</p> <p>The FFIEC previously called this section Electronic- & Paper-Based Media Handling. The revised section now includes discussion on:</p> <ul style="list-style-type: none"> • Data security theory and tools for classifying and protecting data. • Practical application of data classifications and protection files. <p>This includes storage devices such as tapes, laptops, and removable media.</p> <p><i>CSA and MARS work together to help you monitor and control removal of devices that may contain sensitive data.</i></p>				
<p>Security Monitoring</p> <p>The FFIEC renamed Security Testing to Security Monitoring. This emphasizes the need to be proactive with real-time capabilities for managing security. Testing can frequently be viewed as a point-in-time activity performed annually. The stability of the security infrastructure must be monitored continuously. The FFIEC also made significant revisions to this section. Network monitoring practices have significantly matured since the FFIEC’s prior release of this guidance. The new section now provides a comprehensive summary of the components that help create a proactive self-defending network. This section now includes a good review of:</p> <ul style="list-style-type: none"> • Designing the network architecture to support effective monitoring • Network Intrusion Detection Systems • Host Intrusion Detection Systems • Intrusion Detection & Response • Condition Monitoring Tools • Security Testing • Logging <p><i>SDN - The combined capabilities of CSA, NAC, ASA, and MARS allows the institution to establish the necessary network architecture to enable compliance with these updated activity monitoring, analysis, and response guidelines. For example, CSA, ASA, NAC, and MARS work together to deliver security domains, sensor placements at the perimeter and throughout the network, real-time data collection and logging of events, and centralized monitoring and reporting capabilities of all network activity and devices.</i></p>				