Mapping Cisco Security Solutions to ISO 27001

Talhah Jarad
Business Development Manager - Security

© 2010 Cisco and/or its affiliates. All rights reserved.

Mapping Cisco Security Solutions to ISO 27001

Talhah Jarad
Business Development Manager - Security

© 2010 Cisco and/or its affiliates. All rights reserved.

Session Objectives

- In this breakout session we will introduce the concept of standards and frameworks
- This session will provide you with a background on the ISO 27001, its evolution, structure, and benefits
- This session will show you how to prepare your organization for the standard by mapping Cisco technologies to the controls
- We will also discuss the future challenges that need to be taken in considerations

© 2010 Cisco and/or its affiliates. All rights reserved.

Agenda

- Introductions to Standards and Frameworks
- Benefits of the Standards and Frameworks
- ISO 27001 Background
- Applying Cisco Technologies to ISO 27001 Controls
- Recommendations
- Current and Future Considerations

© 2010 Cisco and/or its affiliates. All rights reserved.

Introduction to Standards and Frameworks

© 2010 Cisco and/or its affiliates. All rights reserved.

The Three Pillars of Information Technology

- Process
- People
- Technology (Products)

© 2010 Cisco and/or its affiliates. All rights reserved.

Introduction to Standards and Frameworks

Framework: A set of best practices, a model

Standard: Reference point against which compliance can be evaluated. Basis for comparison

- Alignment: loosely following a framework
- Compliance: Implementing a framework to the letter

- ISO 27002, ISO 17799

- Certification: audited against a standard to be granted its certification

- ISO 27001, ISO 20000

You are following a framework and you are being audited against a standard

© 2010 Cisco and/or its affiliates. All rights reserved.

The Four Main Themes in Compliance

Think “CIAA”

1. Confidentiality — Keep it Secret
2. Integrity of Data — Protect against improper alteration or destruction
3. Availability — Regulated data must be available to authorized users/consumers
4. Audit/Reporting/Monitoring/Logging — Security activity must be tracked/auditable to demonstrate compliance and incident investigation

© 2010 Cisco and/or its affiliates. All rights reserved.

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Introduction to Controls

What are Controls?

- A control is a mechanism (safety measure) that allows delivering value through the management of risks
- IT controls are like the brakes on a car.
- Controls can generate positive results when done correctly.
- Examples

  Quality of Service (QoS)

  Access rule on a firewall

  Network Admission Control (NAC)

© 2010 Cisco and/or its affiliates. All rights reserved.

Benefits of Standards & Best Practices

© 2010 Cisco and/or its affiliates. All rights reserved.

Benefits of the Standards & Best Practices

- Effectiveness and efficiency of IT activities
- Common Language for organization - everyone knows what to do
- Structured –an excellent structure that organizations can follow.
- Expertise - Cumulative years of experience reflected in the models
- Knowledge Sharing – user groups, Web sites, magazines, books
- *Auditable* – to effectively assess control

© 2010 Cisco and/or its affiliates. All rights reserved.

Benefits of the Standards & Best Practices

For Your Reference

- Avoiding re-inventing wheels
- Overcoming vertical silos and nonconforming behavior
- Reducing risks and errors
- Improving quality
- Improving the ability to manage and monitor
- Cost reduction
- Improving trust and confidence from management and partners
- Improve the status and position of the organization

© 2010 Cisco and/or its affiliates. All rights reserved.

Background
ISO 27001

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001 History - BS7799

For Your Reference

- It was originally published by a government department in UK (1999)
- The original standard was issued in two parts:
  - –BS 7799 Part 1: Information Technology – Code of Practice for Information Security Management
  - –BS 7799 Part 2: Information Security Management System – Specification with Guidance for Use
- In 2002 an associated standards, BS7799-2, was published

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001 History - ISO 17799

For Your Reference

- The ISO and IEC, published the international standard ISO 17799: 2000
- This focused upon information security management systems, rather than security controls themselves
- Much more closely aligned with other ISO standards (ISO 9000)
- In 2005, ISO 17799 was re-published to reflect changes in technology.
- Later in the same year, BS7799-2 also became an ISO standard: ISO 27001

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001

For Your Reference

- ISO/IEC 27001 was formerly known as BS7799-2.
- Not a code of practice, like ISO 17799.
- It is the Certifiable Standard
- The Information Security Management standard is now in two (2) updated parts:
  - ISO/IEC 17799: 2005 Code of Practice for Information Security Management
  - ISO 27001: Information Security Management Systems (ISMS) Specification

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001

For Your Reference

- ISO/IEC 17799:2005 Code of Practice for Information Security Management
  - –Basis for developing security standards and management practices
  - –Guidance - Use it as a checklist
  - –No audit against
- ISO/IEC 27001: 2005 ISMS Specification
  - – Certifiable & Auditable
  - –Clauses (4 – 8)
  - – Annex A (5 – 15)

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO/IEC 27003:2010

For Your Reference

- ISO/IEC 27003:2010 focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005.

- It describes the process of ISMS specification and design from inception to the production of implementation plans.

- It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO/IEC 27004:2009

For Your Reference

- ISO/IEC 27004:2009 provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

- ISO/IEC 27004:2009 is applicable to all types and sizes of organization.

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO/IEC 27005:2008

For Your Reference

- ISO/IEC 27005:2008 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

- Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2008.

- ISO/IEC 27005:2008 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27000 Vocabulary

For Your Reference

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001 Format

- 16 Sections
- 11 Security Control Clauses
  - –Annex A (5 – 15)
- 133 security controls
  - – must be covered and an evidence must be shown for each

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001 Format

International Organization for Standardization

Annex A
(normative)

Control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 17799:2005 Clauses 5 to 15. The lists in Table A.1 are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in 4.2.1.

ISO/IEC 17799:2005 Clauses 5 to 15 provide implementation advice and guidance on best practice in support of the controls specified in A.5 to A.15.

Table A.1 – Control objectives and controls

A.5 Security policy		
A.5.1 Information security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27002 (17799) Format

International Organization for Standardization

5 Security policy

5.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

   1) compliance with legislative, regulatory, and contractual requirements;

   2) security education, training, and awareness requirements;

   3) business continuity management;

   4) consequences of information security policy violations;

e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27002 (17799) Sections

1. Scope
2. Terms and Definitions
3. Structure of this Standards
4. Risk Assessment and Treatment
5. Security Policy
6. Organization of Information Security
7. Asset Management
8. Human Resources Security
9. Physical and Environmental Security
10. Communications and Operation Management
11. Access Control
12. Information Systems Acquisitions, Development & Maintenance
13. Information Security Incident Management
14. Business Continuity Management
15. Compliance

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27002 (17799)

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001 Security Controls Clauses

5. Security Policy (2)
6. Organization of Information Security (11)
7. Asset Management (5)
8. Human Resources Security (9)
9. Physical and Environmental Security (13)
10. Communications and Operation Management (32)
11. Access Control (25)
12. Information Systems Acquisitions, Development & Maintenance (16)
13. Information Security Incident Management (5)
14. Business Continuity Management (5)
15. Compliance (10)

© 2010 Cisco and/or its affiliates. All rights reserved.

ISO 27001 Problem Solving Process

For Your Reference

© 2010 Cisco and/or its affiliates. All rights reserved.

Applying Cisco Technologies to ISO 27001 Security Control Clauses

© 2010 Cisco and/or its affiliates. All rights reserved.

Methodology

- The control name and number
- The Objective of the control
- The detailed control clauses numbered as per the standard.
- Cisco Solutions for the detailed control clauses
- Cisco Service will be presented for the controls that require services
- Some non-Cisco will be offered, as deemed necessary
- We will delve in to some of the control clauses in details:
  - Describe the clause, as per the standard
  - Map the clause requirements to Cisco solutions and services

© 2010 Cisco and/or its affiliates. All rights reserved.

A.5 Security Policy

For Your Reference

- A.5.1 Information Security policy

  Objective: to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

  A.5.1.1 Information security policy document

  A.5.1.2 Review of the information security policy

  –Cisco Advanced Services

  - Build Security Policy (Customer Advocacy Services)
  - Governance, Risk management, and Compliance (GRC) Security Assessment Services http://wwwin.cisco.com/CustAdv/services/advtech/security/grc/
  - Security Architecture Assessment (SAA)

  http://collaboratory.cisco.com/confluence/display/CAWIKI/SAA+Ordering+and+Pricing+Detail

© 2010 Cisco and/or its affiliates. All rights reserved.

A.6 Organization of Information Security

For Your Reference

- A.6.1 Internal organization

  Objective: to manage information security within organization.

  A.6.1.1 Management commitment to information security
  A.6.1.2 Information Security co-ordination
  A.6.1.3 Allocation of information security responsibilities
  A.6.1.4 Authorization process for information processing facilities
  A.6.1.5 Confidentiality agreements
  A.6.1.6 Contact with authorities
  –Cisco Advanced Services
  http://wwwin.cisco.com/CustAdv/

© 2010 Cisco and/or its affiliates. All rights reserved.

A.6 Organization of Information Security

For Your Reference

- A.6.1 Internal organization

Objective: to manage information security within organization.

A.6.1.7 Contact with special interest groups

–Cisco Advanced Services

http://wwwin.cisco.com/CustAdv/

–Cisco IntelliShield Alert Manager

– Cisco SIO

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Security Center

For Your Reference

Powered by Intellishield and IronPort SensorBase

Worldwide [change] | Log In | Register | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

Security Center

Inform, Protect, Respond
Early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks

Powered by IntelliShield — Search Security Go — Advanced Search — View Alerts: Most Recent

Security Alert	CVSS Score	Cisco IPS Signature	Cisco PSIRT Advisory	Cisco Applied Mitigation Bulletin	Affected Cisco Products
Adobe Flash Player Multimedia File Integer Overflow Vulnerability HOT	9.3/8.1				
Trojan: TROJ_PGPCODER.A	N/A				
Apache Tomcat Server Improperly Handled Cookie Value Information Disclosure Vulnerability	4.3/3.4				
HP and Sun Java Runtime Environment Applet Handling Arbitrary Code Execution Vulnerability	9.3/6.9				
SIP Protocol Multiple Vulnerabilities	N/A				

> More

» Customize your IntelliShield alerts. Register for a free trial.

Track and Analyze
Threat Analysis and Reporting

Threat Activity Source | Virus Outbreak Level

THREAT ACTIVITY SOURCE

Improve Your Security
Best Practice Guidance

Securing the Data Center
Learn to readdress data center security in the context of newly implemented service-oriented architectures, rich Internet applications, and virtualization.

Security Programs
Methods for improving information and computing asset security

Business Resources
Analysis to guide business decisions

Regulatory Compliance
Ensure networked data confidentiality, integrity, and availability

Design Zone for Security
Tested and validated security designs

Cisco Receives Information Systems Security Award

In recognition of innovation and continued industry leadership, the Information Systems Security Association recently selected Cisco as the Outstanding Organization of the Year for 2007.
Read More

Emergency Response

- Emergency response for network incidents:
  Cisco Technical Support
  800 553-2447 (U.S.)
  Worldwide Contacts
- Urgent assistance for incidents with Cisco products:
  PSIRT
  877 228-7302 (U. S.)
  +1 408 525 6532 (outside U. S.)
- Report an incident involving the Cisco corporate network:
  infosec@cisco.com

Cisco Vulnerability Policy

Security Top of Mind

Enterprise Security Threats and Trends

Cisco Chief Security Officer John N. Stewart and Professor Andrea M. Matwyshyn of The Wharton School at the University of Pennsylvania discuss the business, regulatory, and legal impact of the current network security environment.

© 2010 Cisco and/or its affiliates. All rights reserved.

Intelligence Service Example

For Your Reference

Threat and vulnerability intelligence alerting service

Receive vital intelligence that is relevant and targeted to your Environment

- Tactical, operational and strategic intelligence
- Vendor neutral
- Life cycle reporting
- Vulnerability workflow management system
- Comprehensive searchable alert database

CISCO

IntelliShield

Microsoft Windows DNS Server RPC Interface Buffer Overflow Vulnerability

VULNERABILITY ALERT

Threat Type:	**Unintended Weakness: Buffer Overflow**
IntelliShield ID:	**13092**
Version:	**8**
First Published:	**Apr 13, 2007; 03:20 AM EDT**
Last Published:	**May 10, 2007; 06:31 PM EDT**
Vector:	**Remote**
Authentication:	**Not Required**
Exploit:	**Yes**
Port:	**139, 445, 1024**
CVE:	**CVE-2007-1748**
BugTraq ID:	**23470**

Urgency:	**Possible Use**	3
Credibility:	**Confirmed**	5
Severity:	**Heavy Damage**	5
CVSS Base:	**10.0**	CVSS Calculator CVSS Version 1.0
CVSS Temporal:	**8.7**	

Version Summary: **Avaya has released a security advisory to address the Microsoft Windows DNS server RPC interface buffer overflow vulnerability.**

Description

Microsoft Windows 2000 Service Pack 4 and prior and Windows Server 2003 Service Pack 2 and prior contain a buffer overflow vulnerability that can allow an unauthenticated, remote attacker to execute arbitrary code in the security context of the Domain Name System (DNS) Server Service.

The vulnerability exists in the RPC interface of the DNS Server. An attacker could exploit this vulnerability by sending a crafted RPC packet to an affected system. This action could allow the attacker to execute arbitrary code with *SYSTEM* privileges. An exploit could grant the attacker complete control over an affected system. Control of DNS server systems may allow the attacker to compromise hosts that rely on the DNS server to provide trusted name resolution functionality.

Malicious code exists that is actively exploiting this

Impact

An unauthenticated, remote attacker could exploit this vulnerability to execute arbitrary code with the privileges of the DNS Server, typically *SYSTEM*. Compromises of DNS servers may allow an attacker to launch further attacks against systems that rely on the DNS server to provide trusted name resolution services.

Technical Information

The vulnerability exists due to a lack of bounds checking in the *Lookup_ZoneTreeNodeFromDottedName()* function when calling the *Name_ConvertFileNameToCountName()* function. This function resides in the DNS Server RPC management interface, which is accessible on ports 139/tcp and 445/tcp, as well as random ports above 1024/tcp. The

© 2010 Cisco and/or its affiliates. All rights reserved.

Intelligence Summary Example

For Your Reference

Cisco IntelliShield Cyber Risk Report (CRR)

- A Strategic Intelligence Report that Highlights Current Security Activity and Mid-to Long-range Perspectives
- Addresses seven major risk management categories: vulnerability, physical, legal, trust, identity, human, and geopolitical.
- The CRRs are a result of collaborative efforts, information sharing, and collective security expertise of senior analysts from Cisco security services that include the IntelliShield and IronPort teams

Worldwide [change] Log In | Register | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

IntelliShield Periodic Security Activity Report

April 30–May 6, 2007

Contents

Vulnerability
Physical
Legal
Trust
Identity
Human
Geopolitical
Upcoming Security Activity
Additional Information

The IntelliShield Periodic Security Activity Report (PSAR) is a strategic intelligence product that highlights current security activity and mid- to long-range perspectives. The report addresses seven major risk management categories: vulnerability, physical, legal, trust, identity, human, and geopolitical. The PSARs are a result of collaborative efforts, information sharing, and collective security expertise of senior analysts from Cisco security services that include the IntelliShield team (IntelliShield Alert Manager, Applied Intelligence, and IPS), ROS, PSIRT, the Corporate Security Programs Organization, and Legal Support.

Vulnerability

Although vulnerability and threat activity levels remained low during the time period, there was an increase in the number of new vulnerabilities and issues identified by IntelliShield analysts. This trend was consistent throughout the month of April. Reports of active exploits of the DNS server RPC interface buffer overflow vulnerability in Microsoft Windows described in IntelliShield alert 13092 continued to rise. Alternately, reports of activity related to the ANI file handling arbitrary code execution vulnerability in Microsoft Windows described in IntelliShield alert 12967 are beginning to decline.

Apple released a security bulletin update and updated software to address the Java handling buffer overflow vulnerability in QuickTime. Security researchers that initially discovered the vulnerability also released additional technical details. Although no attacks have been publicly attributed to this vulnerability, IntelliShield analysts recommend applying the updates provided by Apple. This vulnerability was originally demonstrated at the CanSecWest security conference and has received significant media attention since that time.

Cisco released security advisories and updated software to address vulnerabilities in the Cisco Adaptive Security Appliance (ASA) devices and PIX Security Appliance devices. The most serious of these vulnerabilities, which was described in IntelliShield alert 13205, is an authentication bypass vulnerability on devices that use LDAP AAA servers. A device must be configured in one of two ways to be considered vulnerable. The first configuration affects devices that terminate L2TP IPSec tunnels and are configured to use a LDAP authentication server in conjunction with Challenge Handshake Authentication Protocol (CHAP), MS-CHAPv1, or MS-CHAPv2 authentication protocols. The second configuration affects devices that are configured to use a LDAP authentication server to provide AAA services for remote management access, such as telnet, SSH, or HTTP. In either configuration, an attacker could exploit this vulnerability to bypass authentication and access the devices' management interface.

During the time period, Microsoft released information regarding the upcoming May patch release. Seven security bulletins are scheduled for release. Two of these bulletins address vulnerabilities in Microsoft Windows, and three bulletins address vulnerabilities in Microsoft Office. The final two bulletins address vulnerabilities in Microsoft Exchange, CAPICOM, and BizTalk. Microsoft identified several of the vulnerabilities as having a severity rating of critical.

Attackers continued to distribute *W32.Rinbot.A*, and the worm accounted for the majority of malicious code activity during this time period. Antivirus vendors have reported many variations of the worm, many of which have only minor changes, such as filenames, IRC servers, and registry key changes to reflect different executables. This worm has been detected by antivirus vendors as an *Sdbot* variant, *Delbot*, and *Nirbot*.

IntelliShield published 121 events last week; 52 new events and 69 updated events. Of the 121 events, 87 were Vulnerability Alerts, 22 were Security Issue Reports, six were Malicious Code Alerts, five were Daily Virus Reports, and one was a Security Activity Report. The alert publication totals are as follows:

Weekly Alert Totals

Day	Date	New	Updated	Total
Friday	05/04/2007	10	18	28
Thursday	05/03/2007	7	8	15
Wednesday	05/02/2007	18	14	32
Tuesday	05/01/2007	11	7	18

© 2010 Cisco and/or its affiliates. All rights reserved.

Use Your Infrastructure

For Your Reference

Cisco Applied Mitigation Bulletin

Actionable intelligence that can be used with your existing Cisco infrastructure

- Vulnerability Characteristics
- Mitigation Technique Overview
- Risk Management
- Device-Specific Mitigation and Identification
  - Cisco IOS® Routers and Switches
  - Cisco IOS NetFlow
  - Cisco ASA, PIX®, and FWSM Firewalls
  - Cisco ACE Application Control Engine
  - Cisco Intrusion Prevention System
  - Cisco Security Monitoring, Analysis, and Response System

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software and Cisco Unified Communications Manager SIP DoS Vulnerabilities

Document ID: 107966

http://www.cisco.com/warp/public/707/cisco-amb-20080924-sip.shtml

Revision 1.0

For Public Release 2008 September 24 1600 UTC (GMT)

Please provide your feedback on this document.

Contents

Cisco Response
Device Specific Mitigation and Identification
Additional Information
Revision History
Cisco Security Procedures
Related Information

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisories *Multiple Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities* and *Multiple Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerabilities* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

Multiple vulnerabilities exist in specific releases of Cisco IOS Software and Cisco Unified Communications Manager. These vulnerabilities are summarized in the following subsections:

Memory Leak Vulnerability: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through a SIP packet using TCP ports 5060 and 5061 or UDP port 5060. An attacker could exploit this vulnerability using spoofed packets. This vulnerability has been assigned CVE identifier CVE-2008-3799.

Device Reload Vulnerabilities: These vulnerabilities can be exploited remotely without authentication and without user interaction. Successful exploitation of these vulnerabilities may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through SIP packets using TCP ports 5060 and 5061 or UDP port 5060. An attacker could exploit these vulnerabilities using spoofed packets. These vulnerabilities have been assigned CVE identifiers CVE-2008-38800, CVE-2008-3801 and CVE-2008-3802.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisories, which are available at the following links: http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml and http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml.

Mitigation Technique Overview

© 2010 Cisco and/or its affiliates. All rights reserved.

Cyber Security Awareness Website

Cyberspace Action for Education

Keeping Them Safe

Children are exploring online. Help them find a safe and secure path to the digital world.

View information for:

Schools

Higher Ed

Cyberspace Security for All of Us

It takes a village to raise a child. It takes the entire community to work together to keep students, teachers, staff, and families safe online.

Everyone's Responsibility

STOP | THINK | CONNECT

Take action today to make the Internet safer for you, more secure for all.

http://www.cisco.com/go/cafe

Stay Vigilant

Cisco VP and Chief Security Officer John Stewart delivers a 'stop, think, connect' message about protecting yourself online.

Community Effort

Cisco supports NCSA and the October Cyber Security Awareness Month.

Cybersecurity Awareness

Cisco VP Marie Hattar discusses tips for protecting children while using the Internet.

© 2010 Cisco and/or its affiliates. All rights reserved.

Keep These Security Resources Handy

[SAFE Poster]

[Security Annual Report]

[Security Intelligence Operations]

[Secure Borderless Networks]

[Security Solutions Quick Reference Guide]

[Security TrustSec ROI Tool]

© 2010 Cisco and/or its affiliates. All rights reserved.

A.6 Organization of Information Security

- A.6.1 Internal organization

Objective: to manage information security within organization.

A.6.1.8 Independent review of information security

–Cisco Advanced Services

- Security Architecture Assessment (SAA)
  - –Internal SAA, Perimeter SAA, Wireless SAA, UC SAA, DC SAA, Endpoint SAA, Firewall rules assessment, Physical SAA

    http://collaboratory.cisco.com/confluence/display/CAWIKI/SAA+Ordering+and+Pricing+Detail
- Security Posture Assessment (SPA)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.6 Organization of Information Security

For Your Reference

- A.6.2 External Parties

  Objective: to maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties

  A. 6.2.1 Identification of risks related to external parties

  A.6.2.2 Addressing security when dealing with customers

  A.6.2.3 Addressing security in third party agreements

  –Cisco Advanced Services

  - Build security policy
  - Governance, Risk management, and Compliance (GRC) Security Assessment Services

  http://wwwin.cisco.com/CustAdv/services/advtech/security/grc/

© 2010 Cisco and/or its affiliates. All rights reserved.

A.7 Asset management

- A.7.1 Responsibility for Assets

  Objective: to achieve and maintain appropriate protection of organizational assets.

  A.7.1.1 Inventory of assets

  –Switches, routers, wireless access points, IP telephony systems, PCs, laptops, servers, printers, IP cameras, etc.

  –CiscoWorks (element manager)

  –Cisco NAC profiler

  –Cisco Security Manager (CSM)

  –UC/IPT UCMM

  –Cisco Prime

  –Cisco ISE (Identity Service Engine)

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Prime for Enterprise Product Portfolio

- **Cisco Prime Network Control System (NCS)**
- **Cisco Prime LAN Management Solution (LMS)**
- **Cisco Prime Collaboration Manager (CM)**
- **Cisco Prime Network Analysis Module (NAM)**

Simple and Efficient Management Across Architectures, Networks, and Services

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Prime for Enterprise Common Attributes

Optimized Operations Experience

Integrated Cisco Best Practices

Complete Lifecycle Management

Day-One Device Support

Smart Interactions

Physical and Virtual Appliance

Simple and Efficient Management Across Architectures, Networks, and Services

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Prime for Enterprise Common Attributes

Optimized Operations Experience

- Common user interface
- Intuitive user experience
- Optimized operator workflows

Integrated Cisco Best Practices

- Guided deployment of Cisco-validated best practices
- Automated trouble-shooting and diagnostics

Complete Lifecycle Management

- End-to-end lifecycle
- ITIL-aligned operations
- Northbound integration to customer back office

Day-One Device Support

- Support for new devices and technologies upon shipment
- Non-disruptive support upgrades

Smart Interactions

- Context-based help tool
- Real-time access to Cisco support community
- Automated Cisco TAC case creation and management

Physical and/or Virtual Appliance

- Two delivery options
- Both options fully self-contained
- Includes operating system, software application, database, and CLI

© 2010 Cisco and/or its affiliates. All rights reserved.

CiscoWorks

CiscoWorks Resource Management Essentials (RME)

Cisco 2600 Series Multiservice Platforms

Device Name	Updated At	System Description	Location	Contact	Serial Number	Chassis Vendor Type	Total RAM Size (MB)	NVRAM Size (KB)	NVRAM Used (KB)	ROM Version	Total Flash Device Size (MB)
nmtg-cme-2651.cisco.com	Jan 03 2005 12:41:37	Cisco IOS Software, C2600 Software (C2600-IPBASE-M), Version 12.3(4)XD, RELEASE SOFTWARE (fc1) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by Cisco Systems, Inc. Compiled Fri 07-Nov-03 16:39 by eaarmas			JAE073503YM (3192240086)	c2651XM	123.00	26.99	3.87	12.2(7r)	16.00

- GUI
- Reduced human involvement thus errors
- Automates tedious tasks
- Tracks inventory, configs, and software changes

Cisco Systems

24 Hour Inventory Change Report

Generated on Jan 05 2005 10:10:04

Summary

Total number of submitted device(s):	29
Number of device(s) with data:	28
Device(s) with Change:	1

Changes for Device: nmtg-demo-6500-msfc.cisco.com

Memory Pool Identity: MemoryPoolID = 1

Attribute	Type of Change	Time Change Detected	Previous Value	Current Value
Used (MB)	Changed	2005-01-04 14:12:57.323	8422484	8435184
Free (MB)	Changed	2005-01-04 14:12:57.323	24086376	24073712

© 2010 Cisco and/or its affiliates. All rights reserved.

NAC Gap: Non-PC Endpoint Devices

An enterprise LAN is comprised of myriad endpoint types.
Most are undocumented (think DHCP).

Enterprises without VoIP
Wired Endpoints Distribution

Enterprises with VoIP
Wired Endpoints Distribution

© 2010 Cisco and/or its affiliates. All rights reserved.

Examples of Non-PC Endpoints

Printers

Fax Machines

Video Conferencing Stations

IP Phones

Hubs

IP Cameras

Wireless APs

Managed UPS

Cash Registers

Medical Imaging Machines

Alarm Systems

Turnstiles

HVAC Systems

RMON Probes

Vending Machines

. . . and many others

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco NAC Profiler: Automation

Cisco NAC Profiler

PCs	Non-PCs			
	UPS	Phone	Printer	AP

Discovery

Endpoint Profiling

Discover all network endpoints by type and location

Maintain real time and historical contextual data for all endpoints

Monitoring

Behavior Monitoring

Monitor the state of the network endpoints

Detect events such as MAC spoofing, port swapping, etc.

Automated process populates devices into the NAC Manager; and subsequently, into appropriate NAC policy

© 2010 Cisco and/or its affiliates. All rights reserved.

Mapping Profiling to NAC Functions

Authenticate & Authorize

All endpoints are now authenticated

"Authentication" for non-agent devices

MAC Address is to Username as Behavior is to Credential

Quarantine & Enforce

Compromised MAC Addresses or devices are dynamically quarantined

All leverage NAC Appliance policy model for enforcement

Scan & Evaluate

Continuous evaluation and monitoring of endpoint behavior and status

Passive and active techniques

Update & Remediate

Detailed, location-based Help Desk interaction

Ongoing maintenance of the enterprise asset inventory list

© 2010 Cisco and/or its affiliates. All rights reserved.

NAC Profiler Benefits and Overview

Discovery

Endpoint Profiling
Discover all network endpoints by type and location.

Monitoring

Device Monitoring
Maintain real-time and historical contextual data for all endpoints.

Categorization Profiling Example

Cisco IP Phone

HP Printer

Cisco Surveillance Camera

UPS

Nonsupplicant-Aware OS

© 2010 Cisco and/or its affiliates. All rights reserved.

Introducing Identity Services Engine

Next Generation Solution Portfolio

Identity & Access Control

Identity & Access Control + Posture

Device Profiling & Provisioning + Identity Monitoring

Guest Lifecycle Management

Access Control Solution

NAC Manager

NAC Server

NAC Profiler

NAC Collector

Standalone appliance or licensed as a module on NAC Server

NAC Guest Server

ISE

NAC Agent

© 2010 Cisco and/or its affiliates. All rights reserved.

A.7 Asset management

- A.7.1 Responsibility for Assets

  Objective: to achieve and maintain appropriate protection of organizational assets.

  A.7.1.2 Ownership of assets

  –Partially through Role/Rule Based Access Control

  –Cisco Security Manager (CSM)

  –Cisco ACS (AAA) /ISE

  –Cisco TrustSec (CTS)

  –Cisco Advanced Services (Documentation)

© 2010 Cisco and/or its affiliates. All rights reserved.

CSM Managed Device Families

Firewall
VPN
IPS

ASA 5500 Series

AIP-SSM

3000 and 4000 Series Switches

IDSM-2

FWSM

VPN SPA

IPS 4200 Series

Catalyst 6500 Series

7600 Series

IPS AIM

Integrated Services Routers (800, 1800, 2800, 3800 Series)

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Security Manager

Integrated Security Configuration Management

Firewall Management

- Support for Cisco® PIX® Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), and Cisco IOS® Software Routers
- Rich firewall rule definition: shared objects, rule grouping, and inheritance
- Powerful analysis tools: conflict detection, rule combiner, hit counts, …

VPN Management

- Support for Cisco PIX Firewall, Cisco ASA, VPN services module (VPNSM), VPN shared port adapter (SPA), and Cisco IOS Software routers
- Support for wide array of VPNtechnolgies, such as DMVPN, Easy VPN, and SSLVPN
- VPN wizard for 3-step point-and-click VPN creation

IPS Management

- Support for IPS sensors and Cisco IOS IPS
- Automatic policy-based IPS sensor software and signature updates
- Signature update wizard allowing easy review and editing prior to deployment

Productivity

- Unified security management for Cisco devices supporting firewall, VPN, and IPS
- Efficient management of up to 5000 devices per server
- Multiple views for task optimization
  - Device view
  - Policy view
  - Topology view

© 2010 Cisco and/or its affiliates. All rights reserved.

A.7 Asset management

- A.7.1 Responsibility for assets

  Objective: to achieve and maintain appropriate protection of organizational assets.

  A.7.1.3 Acceptable use of assets

  -NAC – Acceptance Usage Policy (AUP)

  -WSA (Iron Port) AUP

  -Cisco GRC (Governance, Risk, Compliance)

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco WSA (IronPort)

A Powerful, Secure Web Gateway Solution

- Most effective defense against web-based malware
- Visibility and control for acceptable use and data loss
- High performance to ensure best end-user experience
- Integrated solution offering optimum TCO

© 2010 Cisco and/or its affiliates. All rights reserved.

Critical Acceptable Use Reports

- Real-time insights
  - Visibility into web usage and trends
  - Monitor acceptable use trends
  - Identify risky user behavior

- Extensive Forensic Capabilities
  - Investigate acceptable use violations
  - Drill down for further analysis
  - Satisfy compliance requirements

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco WSA (IronPort) URL Filters

Comprehensive Management and Visibility

- Flexible policy management
  - Per user, per group policies
  - Multiple actions, including block, warn and monitor
  - Time-based policies
  - Custom categories and notifications
  - Guest Policies
- Visibility
  - Easy-to-understand reports
  - Extensive logging
  - Comprehensive alerting

© 2010 Cisco and/or its affiliates. All rights reserved.

A.7 Asset management

- A.7.2 Information classification

  Objective: to ensure that information receives an appropriate level of protection

  A.7.2.1 Classification guidelines

  A.7.2.2 Information labeling and handling

  –MPLS Tagging

  –VLANs

  –QoS (DSCP/IP precedence)

  –WSA and ESA (IronPort)

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Content Security WSA and ESA (IronPort®) Gateway Security Products

Web Security **Email Security** **Security Management** **Encryption**

© 2010 Cisco and/or its affiliates. All rights reserved.

The IronPort SenderBase® Network Global Reach Yields Benchmark Accuracy

- **30B+** queries daily
- **150+** Email and Web parameters
- **25%** of the World's Traffic
- Cisco Network Devices

- View into **both** email & Web traffic dramatically improves detection
- 80% of spam contains URLs
- Email is a key distribution vector for Web-based malware
- Malware is a key distribution vector for Spam zombie infections

Combines Email & Web Traffic Analysis

© 2010 Cisco and/or its affiliates. All rights reserved.

Increasing Enterprise Web Traffic

Ubiquitous Path In and Out of Enterprise Networks

HTTP is the New TCP

- Growing business web usage
- Growing tunneled apps usage

© 2010 Cisco and/or its affiliates. All rights reserved.

Web Application Control

- Native control for HTTP, HTTPs, FTP applications
- Selective decryption of SSL traffic for security and policy
- Policy enforcement for applications tunneled over HTTP—FTP, IM, video
- Application traversal using policy-based HTTP CONNECT

© 2010 Cisco and/or its affiliates. All rights reserved.

A.8 Human Resources Security

For Your Reference

- A.8.1 Prior To Employment

Objective: to ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

A.8.1.1 Roles and responsibilities

A.8.1.2 Screening

A.8.1.3 Terms and conditions of employment

–Cisco Advanced Services (to create policies)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.8 Human Resources Security

- A.8.2 During Employment

  Objective: to ensure that all employees, contractors, and third party users are aware of the information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy I the course of their normal work, and to reduced the risk of human error.

  A.8.2.1 Management responsibilities

  A.8.2.2 Information security awareness, education and training

  –CCSP, CCIE for technical staff, CISSP, Security+

  –Cisco Security Intelligence Operations (SIO)

  –Cisco Digital Media Signage

  –Cisco Webex (online and recorded sessions)

  –Cisco TelePresence and Tandberg Solutions

  –Cisco Advanced Services

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco SIO
Key Components

For Your Reference

Powerful Ecosystem Enables Fast, Accurate Protection

Cisco SensorBase

- World's biggest, broadest and best traffic monitoring network

Cisco Threat Operations Center

- Global operation provides high responsiveness and accuracy

Advanced Protection

- Dynamic updates and actionable intelligence ensure fast, accurate protection

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Threat Operations Center

Sophisticated Security Modeling and Remediation

For Your Reference

- **Advanced algorithms**
  - Dynamic real-time scoring
  - Fast threat identification
  - Automated rule and/or signature creation
  - Human-aided rule creation
- **White Hat engineers**
  - Penetration testing
  - Botnet infiltration
  - Malware reverse engineering

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Digital Media Signage

- The Cisco Digital Media System solution suite comprises products for the creation, management and access of digital media.
- Integrate the video surveillance system with the Cisco Unified Communications system and Cisco digital signage system

© 2010 Cisco and/or its affiliates. All rights reserved.

A.8 Human Resources Security

For Your Reference

- A.8.2 During Employment

  Objective: to ensure that all employees, contractors, and third party users are aware of the information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy I the course of their normal work, and to reduced the risk of human error.

  A.8.2.3 Disciplinary process

  –Cisco Advanced Services (create policies)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.8 Human Resources Security

- A.8.3 Termination or Change of Employment

  Objective: to ensure that employees, contractors, and third party users exit an organization or change management in an orderly manner.

  A.8.3.1 Termination responsibilities

  A.8.3.2 Return of assets

  –RFID Tagging

  A.8.3.3 Removal of access rights

  –Cisco ACS (AAA) /Cisco ISE

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Access Control System (ACS)

TACACS+

- Change Password
- Custom Attributes
- Custom Services

Identity Stores

- RSA SecurID
- Token Servers
- RADIUS Proxy

Protocols

- EAP-FAST with GTC inner
- PEAP with GTC inner
- LEAP
- CHAP
- MS-CHAPv1
- MS-CHAPv2

Admin

- New Roles
- Cert Enhancements
- Access Restrictions
- Password Enhancements
- Web Services & Scripting

Policy

- Network Access Restrictions (NARs)
- Default Device Definition
- EAP-TLS Cert comparison against AD

Monitoring and Troubleshooting

- Customizable Dashboard
- Syslog Event Notification
- Expert Troubleshooter
- New Catalog Reports
- Data Export

© 2010 Cisco and/or its affiliates. All rights reserved.

Policy for Access and Administration

Network Access

Authenticate users to the network

Apply per user policies

Audit & report on network access

Device Administration

Authenticate users to network devices

Control levels of access to commands

Audit & report on configuration changes

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco ACS Integration

For Your Reference

© 2010 Cisco and/or its affiliates. All rights reserved.

Monitoring and Reporting

For Your Reference

Alarms and Notifications

- Custom Triggers
- Alerts via Email and Syslog

Comprehensive Reporting

- Standard Reports
- Templates
- Customized Reports

Fully Configurable Dashboard

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

- A.9.1 Secure Areas

  Objective: to prevent unauthorized physical access, damage and interferences to the organization's premises and information.

  A.9.1.1 Physical security perimeter

  -Cisco Video Surveillance Solution

  -Cisco Video Surveillance Manager (VSM)

  -Cisco Video Surveillance Operation Manager (VSOM)

  -Cisco Video Surveillance Virtual Matrix (VSVM)

  -Cisco IP Cameras

  -Cisco Video Surveillance Storage

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Security Solution Components

- **Video Encoders/IP Cameras**
- Source of digital video over IP.
- Compressed MJPEG, MPEG2, MPEG4.

- **Video and Application Servers**
- Linux servers for streaming video between cameras, storage and viewers. May also run a Web server or application sever for delivering a Web application.

- VSMS – VSOM - VSVM

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Security Solution Components

- Network
- TCP/IP network, typically on Ethernet.
- Conventional switches and routers.

- Storage
- Redundant RAID storage
- Direct Attached, SAN or iSCSI

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Security Solution Components

- **Client Stations**
- Windows PCs for video decoding, display and control.
- Running Web browsers or specialized Windows applications.

© 2010 Cisco and/or its affiliates. All rights reserved.

Video Display

- Provides real-time remote monitoring w/virtual matrix switching (VSVM)
- Display live and archived video streams with high quality images.
- PTZ control and presets
- Review and clip archives

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

- A.9.1 Secure Areas

  Objective: to prevent unauthorized physical access, damage and interferences to the organization's premises and information.

  A.9.1.2 Physical entry controls

  - Cisco Physical Access Control

  A.9.1.3 Securing offices, rooms, and facilities

  - Cisco Physical Access Control

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Access Gateways

- Connects door locks and readers to the IP network
- Controls up to thousands of doors
- Directly configurable through a built-in Web server
- Supports offline operations if network connectivity is lost
- 250,000 credentials can be cached and encrypted
- 150,000 events can be buffered by the door

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Access Manager

- Management application for configuring hardware, monitor activity, and enroll users
- Supports a comprehensive list of access control policies
- Easy integration with other IT systems
- Flexible reporting capability
- Easy access to video through integration with Cisco Video Surveillance Manager

Quick Launch Bar, Integrated Video

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Access Manager

- New Form factor

  Software can be ordered on new MSP 1RU servers, simplifying ordering & deployment

- Web Services API

  Optional Web Services API to provide programmable access from any client application

  PSIM Integration: Integration with Proximex

  Visitor Management Integration: API for easy integration with visitor management applications

- Bulk Image upgrade

  Allows flexible firmware upgrade for all or a group of hardware devices, thereby lowering TCO

- Usability improvements

© 2010 Cisco and/or its affiliates. All rights reserved.

Electronic Access Control architectures today….

- Complex & expensive to design, deploy and maintain
- Not capable of incremental deployment : Upfront design cycle required
- Separate power circuit required to power door hardware

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Access Control Overview

•A Comprehensive Solution for Electronic Access Control
•Leverages IP infrastructure, integrates with other Physical Security applications

- Hardware:

  Cisco Access Gateway connects existing door hardware (readers locks etc.) to the network

  Additional doors can be managed by connecting expansion modules to the Access Gateway

- Software

  Cisco Physical Access Manager (Cisco PAM) is a Management Appliance for configuration, monitoring and report generation.

© 2010 Cisco and/or its affiliates. All rights reserved.

Deployment Architecture

Scalable Modular Architecture, easily integrated with IT application data

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Physical Access Manager (Cisco PAM)

- 1 RU Appliance
- Java Thin Client Architecture
- Policy Support: Two-Door, Anti-Passback
- Report Generator (Canned & Custom)
- Badge Design & Enrollment
- Microsoft Active Directory integration
- Fine grained user rights
- Global I/O
- Device Pre-Provisioning
- Capacity & Feature Licenses
- IT Data integration
- Warm Standby High Availability
- Audit Trails

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco PAM High Availability

- Warm standby with database replication between two Cisco PAM instances
- Virtual IP address for client transparency: both IP addresses bonded to a single virtual IP address
- Secondary server takes over when primary fails
- Secondary server only requires a HA license: acquires all primary licenses

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Video Surveillance Manager (VSM) integration

- Event Video integration with Cisco VSM
- Dynamically acquires camera inventory stored in Cisco VSM. Automatically tracks inventory.
- Allows association of cameras to doors.
- For every event by the door, recorded and live video can be viewed, PTZ presets can be changed.

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

- A.9.1 Secure Areas

  Objective: to prevent unauthorized physical access, damage and interferences to the organization's premises and information.

  A.9.1.4 Protecting against external and environmental threats

  A.9.1.5 Working in secure areas

  -Cisco physical access control

  -Cisco video surveillance solution

  -Cisco Cameras

  -Cisco IPICS

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IPICS

- Cisco Interoperability and Collaboration System is an intelligent resource management application that orchestrate resources, media, and information
- IPICS consists of
  -IPICS Server
  -Land Mobile Radio Gateways
  -Push-to-Talk Media Clients
  -Cisco IP Phone PTT Clients
  -Cisco Policy Engine
- Effectively manage communications across distributed radio systems, locations, and networks.

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IP Phones and IPICS

- The IPICS XML IP-Phone client provides Push-to-Talk service for Cisco IP phones
- Secure access to radio PTT talkgroups and channels from anywhere in the UC network
- Available on a wide range of IP-phones including wireline and WiFi IP-phones
- Intuitive user interface with smooth transition between telephony and radio communications

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IPICS for Incident Response

For Your Reference

- Cisco Interoperability and Collaboration System (IPICS) takes incident response to the next level
- IPICS allows multiple safety and security organizations to quickly share vital incident information, including live mobile video, across previously isolated radio networks
- IPICS integrates with Cisco Video Surveillance, Cisco Physical Access Control, and third-party applications, further enhancing situational awareness, response time, operational efficiency and cross-agency collaboration during a critical event

© 2010 Cisco and/or its affiliates. All rights reserved.

IPICS Server

- New Form factor
  - Software can be ordered on new MSP 1RU servers, simplifying ordering & deployment
- High Availability improving 24/7 reliability
  - Active/standby servers providing no single point of failure within IPICS solution
  - Can be co-located or geographically distributed (minimum T1)
- Loop prevention of patches
- Radio pooling
  - Can pool serial and tone controlled radios so that dispatchers simply select channels
  - Improved TCO/ ROI from fewer radio and networking resources

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IPICS Dispatch Console

Unified Communications Command and Control

For Your Reference

- Communicate with on-site personnel using all media
- Push video, images and data to first responders
- Collaborate with first responders and other organizations
- Use with any radio network for smooth evolution to new radio protocols (P25, Tetra)

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IPICS Mobile Client

Situational awareness and collaboration

For Your Reference

- App for Apple iPhone
- Integrated PTT w/Radio interoperability
- Rich-media incident management
  - Increased Situational Awareness
  - Increased Collaboration – Citizens / Others
  - View Incidents, status, media
  - Receive / send video, images
- 3G and WiFi Support
- Secure access

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

For Your Reference

- A.9.1 Secure Areas

  Objective: to prevent unauthorized physical access, damage and interferences to the organization's premises and information.

  A.9.1.6 Public access, delivery and loading areas

  -Cisco physical access control

  -Cisco Video surveillance solution

  -Cisco Cameras

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

For Your Reference

- A.9.2 Equipment Security

  Objective: to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities

  A.9.2.1 Equipment sitting and protection

  – RFID

  A.9.2.2 Supporting utilities

  – Air Conditioning (AC), Uninterruptible Power Supply (UPS), power supply, data center setup

  A.9.2.3 Cabling security

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

For Your Reference

- A.9.2 Equipment Security

  Objective: to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities

  A.9.2.4 Equipment maintenance

  – GOLD, EEM, CallHome Alerts

  –SMARTnet, Smart Care, and other Cisco maintenance services

  –IBLM (Install Base Lifecycle Management)

© 2010 Cisco and/or its affiliates. All rights reserved.

Smart Call Home

© 2010 Cisco and/or its affiliates. All rights reserved.

A.9 Physical and Environmental Security

For Your Reference

- A.9.2 Equipment Security

  Objective: to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities

  A.9.2.5 Security of equipment off-premises

  A.9.2.6 Secure disposal or re-use of equipment

  A.9.2.7 Removal of property

  – RFID

  –Cisco Video surveillance solution

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management

For Your Reference

- A.10.1 Operational Procedures and Responsibilities

  Objective: to ensure the correct and secure operation of information processing facilities

  A.10.1.1 Documented operating procedures

  – Cisco Advanced Services

  A.10.1.2 Change management

  – ACS (access side)

  –CSM (approval process)

  –CiscoWorks

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management

For Your Reference

- A.10.1 Operational Procedures and Responsibilities

  Objective: to ensure the correct and secure operation of information processing facilities

  A.10.1.3 Segregation of duties

  – Cisco ACS and using RBAC

  – Cisco NAC

  –.1x

  –Cisco TrustSec

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management

- A.10.1 Operational Procedures and Responsibilities

  Objective: to ensure the correct and secure operation of information processing facilities

  A.10.1.4 Separation of development, test, and operational facilities

  – VLANs

  –DMZs

  –Virtualization

  –ASA – Virtual Firewalls

  – Cisco IOS Zone Based Firewall

  –Nexus 1000v

  –MPLS VPN and VRFs

© 2010 Cisco and/or its affiliates. All rights reserved.

Using VLANs for Access Control

- Dynamic VLAN assignment
- Dynamic security policy assignment using ACLs
- Identity Networking-based user/port accounting

© 2010 Cisco and/or its affiliates. All rights reserved.

ASA - Virtual Firewalls

- Virtual firewall—when a single firewall device can support multiple contexts
- A context defines connected networks and the policies that the firewall enforces
- Security policies (ACL, NAT, app inspection)
  - IP address space (overlapping permitted across contexts)
  - An operational mode: either routed **or** transparent
- Virtual firewall allows a device to enforce many (up to 100s) policies between different networks
- Caveat is that virtual often means smaller as processing power of all the virtual firewall adds up to the original appliance

© 2010 Cisco and/or its affiliates. All rights reserved.

Virtual Firewall Overview

For Your Reference

Context Hierarchy

- Inside a context, almost all features are virtualized, e.g., one context can syslog to IP 10.10.50.1 while another context sends syslog only for severity 3 messages to IP 192.168.1.5

© 2010 Cisco and/or its affiliates. All rights reserved.

Highly Scalable Multicontext Security Services

For Your Reference

- Security contexts (virtual firewalls) lower operational costs
- Reduce overall management and support costs by hosting multiple virtual firewalls in a single appliance
  - Enables the logical partitioning of a single Cisco ASA security appliance into multiple logical firewalls, each with their own unique policies and administration
  - Each context provides the same primary firewall features provided by a standalone Cisco PIX Security Appliance
  - Supports up to 100 contexts, depending on platform
- Ideal solution for enterprises consolidating multiple firewalls into a single larger appliance, or service providers who offer managed firewall or hosting services

© 2010 Cisco and/or its affiliates. All rights reserved.

Enterprise Security Zones—Logical

© 2010 Cisco and/or its affiliates. All rights reserved.

Enterprise Security Zones—Physical

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IOS Zone-Based Policy Firewall

- Allows grouping of physical and virtual interfaces into zones
- Firewall policies are applied to traffic traversing zones
- Simple to add or remove interfaces and integrate into firewall policy

Supported Features

- Stateful Inspection
- Application inspection: instant message, POP, IMAP, SMTP/ESMTP, HTTP
- URL filtering
- Per-policy parameter
- Transparent firewall
- VRF-aware firewall

© 2010 Cisco and/or its affiliates. All rights reserved.

Deployment Locations – Separation

© 2010 Cisco and/or its affiliates. All rights reserved.

Server Virtualization Issues

1. vMotion moves VMs across physical ports—the network policy must follow

2. Impossible to view or apply network policy to locally switched traffic

3. Need shared nomenclature and collaboration for security policies between network and server admin

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Nexus 1000V

- Industry's most advanced software switch for VMware vSphere
- Built on Cisco NX-OS
- Compatible with all switches
- Compatible with all servers on the VMware Hardware Compatibility List
- Winner of VMworld Best in Show 2008 and Cisco Most Innovative Product of 2009

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management

For Your Reference

- A.10.2 Third Party Service Delivery Management

  Objective: to implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements

  A.10.2.1 Service delivery

  –Cisco Advanced services

  A.10.2.2 Monitoring and review of third party services

  –IPS (for data transmission)

  –Cisco Advanced Services (Audit)

  A.10.2.3 Managing changes to third party services

  – IBM Tivoli or HP OpenView

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management

- A.10.3 System Planning and Acceptance

  Objective: to minimize the risk of systems failures

  A.10.3.1 Capacity management

  –NAM (Network Analysis Module)

  –Netflow technology

  – Cisco EnergyWise for energy consumption and optimization

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco EnergyWise

Converges IT and facility networks

- Innovative solution on Cisco Catalyst switching and routing portfolio
- Enables reduction of greenhouse gas (GhG) emissions
- Drives significant cost savings
- Monitors, reports, and reduces energy usage across entire business
- Manages PoE network devices as well as desktop and laptop
- Provides compelling reports for policy optimization, troubleshooting, and demonstration of energy

"Forrester analyst Doug Washburn said the initiative comes at a good time as companies are looking to go both green and also cut costs. If they get on board, he said, there could be some significant savings beyond IT."

– Ryan Kim, San Francisco Chronicle

"'Going green has been an industry buzzword for the past couple of years, but Cisco Systems …put its money where its mouth is to help organizations chop energy costs and reduce their carbon footprints with software that can manage devices and systems that gobble up power."

– Andrew Hickey, CRN Canada Online

© 2010 Cisco and/or its affiliates. All rights reserved.

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Confidential

A.10 Communication and Operations Management

For Your Reference

- A.10.3 System Planning and Acceptance

  Objective: to minimize the risk of systems failures

  A.10.3.2 System acceptance

  –Services (Staging) from Cisco or partner

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.4 Protecting Against Malicious and Mobile Code

Objective: to protect the integrity of software and information

A.10.4.1 Controls against malicious code

–Cisco NAC solution

–Cisco IPS

–WSA and ESA (Iron Port)

–Botnet filter (on ASA)

–Global correlation (on IPS)

–Netflow for anomaly

–Cisco Intellishield

© 2010 Cisco and/or its affiliates. All rights reserved.

Detecting Client Infections

Botnet Traffic Filter on ASA 5500 Series

- Monitors malware traffic
  - Scans all traffic, ports & protocols
  - Detects infected clients by tracking rogue "phone home" traffic
- Highly accurate
  - Identifies100,000s of malware connections per week
  - Automatic DNS lookups of addresses
  - Dynamic database integrated into Cisco Security Intelligence Operations

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Botnet Traffic Filter Reports

Top Botnet Sites, Ports and Infected Endpoints

Monitoring

Live Dashboard

Integrated Reporting

© 2010 Cisco and/or its affiliates. All rights reserved.

IPS Reputation Filtering

Significantly Increasing Accuracy

- Powerful preventive defense
  - Blocks 20% of threats before attacks occur (micro to macro)
- Two-way policy decision
  - Block “known bad” traffic
  - Pass other traffic to the next stage for further inspection
- Real-time updates

Cisco IPS has TWICE the IPS deployments of any other vendor

© 2010 Cisco and/or its affiliates. All rights reserved.

Tackling Malware: Solutions Across the Network

© 2010 Cisco and/or its affiliates. All rights reserved.

Tackling Malware: Solutions Across the Network

© 2010 Cisco and/or its affiliates. All rights reserved.

Global Correlation in Action

Network IPS to Global IPS

For Your Reference

08:00 GMT

- A sensor in Australia detects new malware
- A sensor in Russia detects a botnet issuing new commands
- A sensor in Korea detects a virus mutating
- A sensor in Florida detects a hacker probing major financial institutions

Fast, Complete & Accurate Protection Using Global IPS Data

08:15 GMT

- All Cisco IPS customers protected

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.4 Protecting Against Malicious and Mobile Code

  Objective: to protect the integrity of software and information

  A.10.4.2 Controls against mobile code

  –Cisco secure Desktop CSD

  –Cisco AnyConnect

  –Cisco IPS

  – Cisco WSA and ESA (IronPort web and mail filtering)

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Desktop

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.5 Back-up

  Objective: to maintain the integrity and availability of information and information processing facilities

  A.10.5.1 Information back-up

  –Storage replication solution

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.6 Network Security Management

  Objective: to ensure the protection of information in networks and the protection of the supporting infrastructure

  A.10.6.1 Network controls

  – Cisco ASA

  – Cisco IPS

  –VPN

  – Cisco WSA and ESA (IronPort)

  –Borderless Networks security approach

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Adaptive Security Appliance

Industry's Most Proven Firewall

- Most widely deployed network security platform
  - Millions of devices deployed
  - 100,000s of installations
- High performance, adaptive solution
- 15 years of investment, 1,000s of security engineers
- Common Criteria EAL4+; industry's broadest coverage

Cisco Adaptive Security Appliances

Granular Access Controls

Advanced Threat Protection

Secure Connectivity

Secure Unified Communications

Comprehensive Management

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Architecture for the Advanced Next Generation Firewall

© 2010 Cisco and/or its affiliates. All rights reserved.

Adaptive Security Appliance Platform

Powerful Market-Proven Capabilities

- High-performance, scalable platform
- Enterprise-class availability
- Intelligent networking services
- Virtualized and transparent operations

© 2010 Cisco and/or its affiliates. All rights reserved.

Enterprise-Class Availability
Maximizing Uptime

High Availability

- Full-meshed Active/Standby and Active/Active
- Full application state synchronization
- Zero downtime upgrades
- Sub-second failover

Reliability & Resilience

- 2X reliability of a server-based solution

  Typical server: 50-65K hrs*

  Cisco ASA: 100-150K hrs*
- Redundant power supplies
- Multi-level resiliency prevents component, link, system failure

* MTBF calculation based on Telcordia (Bellcore) SR-332.

© 2010 Cisco and/or its affiliates. All rights reserved.

Versatile Deployments
Virtual Firewalls and Transparent Operation

Virtual Firewalls

- Fully virtualized ASA contexts
- Enables device consolidation & segmentation
- Supports separate policies & administration

Transparent Operation

- Operates at layer 2, transparent to the network
- Drops into existing networks without re-addressing
- Simplifies internal firewalling & network segmentation

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.6 Network Security Management

  Objective: to ensure the protection of information in networks and the protection of the supporting infrastructure

  A.10.6.2 Security of network services

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.7 Media Handling

  Objective: to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities

  A.10.7.1 Management of removable media (note procedures)

  – CSD, SME (Storage Media Encryption)

  A.10.7.2 Disposal of media

  –CSD, SME (Storage Media Encryption)

  A.10.7.3 Information handling procedures

  –CSD, SME (Storage Media Encryption)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.7 Media Handling

  Objective: to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities

  A.10.7.4 Security of system documentation

  –Cisco Secure Desktop (CSD)

  –IronPort

  –SME (Storage Media Encryption)

  –ACS for logical access/ ISE

  –Cisco physical security solution for physical access

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.8 Exchange of Information

Objective: to maintain the security of information and software exchanged within an organization and with any external entities

A.10.8.1 Information exchange policies and procedures

A.10.8.2 Exchange agreements

A.10.8.3 Physical media in transit

A.10.8.4 Electronic messaging

–ESA (IronPort) email encryption

–SSL VPN

–ASA (application inspection)

© 2010 Cisco and/or its affiliates. All rights reserved.

Protocol Inspection on Cisco ASA Firewall

Application Layer Protection

- Application-aware inspection
  - Strong security
  - Granular policy controls
- Application-layer controls
  - Perform conformance checking
  - State tracking
  - Security checks and more
- Over 30 inspection engines

Unified Communications

SIP
SCCP (Skinny)
H.323 v1–4
GTP (3G Mobile Wireless)
MGCP
TRP/RTCP/RTSP
TAPI/JTAP

Database & OS Services

Oracle/SQL*Net (V1/V2)
Microsoft RPC/DCE RPC
NFS
ILS/LDAP
Sun RPC/NIS+

Core Protocol Support

HTTP/HTTPS
FTP/TFTP
SMTP/ESMTP
DNS/EDNS
TCP/UDP

Enterprise Applications

Microsoft Windows Messenger
Microsoft NetMeeting
Real Player
Cisco IP Phones
Cisco SoftPhones

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.8 Exchange of Information

Objective: to maintain the security of information and software exchanged within an organization and with any external entities

A.10.8.5 Business information systems

–Cisco Services

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.9 Electronic Commerce Services

  Objective: to ensure the security of electronic commerce services, and their secure use

  A.10.9.1 Electronic commerce

  –SSL

  –VPN

© 2010 Cisco and/or its affiliates. All rights reserved.

Comprehensive Endpoint Security for Cisco SSL VPN Solution

Complete Pre-Connect Assessment:

- **Location Assessment**—Managed or Unmanaged Desktop?
- **Security Posture Assessment**—Is AV Operational/Up-to-Date, Personal Firewall Operational, Malware Present?

Comprehensive Session Protection:

- Data Sandbox and Encryption Protects Every Aspect of Session
- Malware Detection with Hooks to Microsoft Free Anti-Spyware Software

Post-Session Clean-Up:

- Encrypted Partition Overwrite (not just Deletion) Using DoD Algorithm
- Cache, History, and Cookie Overwrite
- File Download and E-mail Attachment Overwrite
- Auto-Complete Password Overwrite

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.9 Electronic Commerce Services

  Objective: to ensure the security of electronic commerce services, and their secure use

  A.10.9.2 On-Line transactions

  –SSL and IPSec VPN

  A.10.9.3 Publicly available information

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.10 Monitoring

  Objective: to detect unauthorized information processing activities

  A.10.10.1 Audit logging

  –ACS (accounting part)

  A.10.10.2 Monitoring system use

  –Cisco Services DLP Audit

  –IPS Audit

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

For Your Reference

- A.10.10 Monitoring

  Objective: to detect unauthorized information processing activities

  A.10.10.3 Protection of log information

  –SME

  A.10.10.4 Administrator and operator logs

  –Enable logging on devices. Use ACS for accounting

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.10 Monitoring

  Objective: to detect unauthorized information processing activities

  A.10.10.5 Fault logging

  –Cisco Security Manger CSM

  –CiscoWorks

© 2010 Cisco and/or its affiliates. All rights reserved.

A.10 Communication and Operations Management (Cont'd)

- A.10.10 Monitoring

  Objective: to detect unauthorized information processing activities

  A.10.10.6 Clock synchronization

  –Enable NTP on all Cisco devices

© 2010 Cisco and/or its affiliates. All rights reserved.

Network Time Protocol

- Synchronize time across all devices
- When security event occurs, data must have consistent timestamps
  - From external time source (Upstream ISP, Internet, GPS, atomic clock)
  - From internal time source
  - Router can act as stratum 1 time source

```
ntp source loopback0
ntp server 10.1.1.1 source loopback0
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Network Time Protocol Security

- Authenticate NTP messages
- NTP access controls

  http://www.cisco.com/warp/public/707/cisco-sa-20020508-ntp-vulnerability.shtml#workarounds
- Disable NTP on interfaces that don't need it

```
ntp authenticate
ntp authentication-key 1 md5 <value>
ntp trusted-key 1
ntp access-group {query-only | serve-only | serve |
peer} <ACL number>
Interface fa0/0
  ntp disable
```

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.1 Business requirement for access controls

  Objective: to control access to information

  A.11.1.1 Access controls policy
  - Cisco GRC
  - Cisco Services (to create policies)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.2 User Access Management

  Objective: to ensure authorized user access and to prevent unauthorized access to information systems.

  A.11.2.1 User registration

  –Process and Cisco ACS

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.2 User Access Management

  Objective: to ensure authorized user access and to prevent unauthorized access to information systems.

  A.11.2.2 Privilege management

  – Cisco ACS / ISE

  –Cisco TrustSec

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco TrustSec

- Cisco TrustSec is a security solution that provides
  - Policy-based access control
  - Identity-aware networking, and
  - Data integrity and confidentiality services

- The term TrustSec has been expanded to include several methods for securing network access and control, including:
  - Switch infrastructure solutions
  - Identity-Based Networking Services
  - 802.1X
  - Security Group Tags (SGTs)

- Appliance-based solutions:
  - Network Admission Control

© 2010 Cisco and/or its affiliates. All rights reserved.

Key TrustSec Functions

Policy-based access control for

- Users
- Endpoint devices (posture)
- Networking infrastructure

Identity-aware networking

- Identity information for granular controls
- Role-based business service delivery

Data integrity and confidentiality

- Securing data path in the switching environment
- IEEE 802.1AE standard encryption

© 2010 Cisco and/or its affiliates. All rights reserved.

Changing Business Environment Drives Network Access Control Demands

© 2010 Cisco and/or its affiliates. All rights reserved.

Customer Challenge in Building an Access Policy in a Borderless Network

Common questions organizations ask

Authorized Access

- How can I restrict access to my network?
- Can I manage the risk of using personal PCs?
- Common access rights when on-premises, at home, on the road?
- Endpoints are healthy?

GuestAccess

- Can I allow guests Internet-only access?
- How do I easily create a guest account?
- Can this work in wireless and wired?
- How do I monitor guest activities?

Non-Authenticating Devices

- How do I discover non-authenticating devices?
- Can I determine what they are?
- Can I control their access?
- Are they being spoofed?

© 2010 Cisco and/or its affiliates. All rights reserved.

Authentication and Authorization

Vicky Sanchez
Employee, Marketing
Wireline
3 p.m.

Frank Lee
Guest
Wireless
9 a.m.

Security Camera G/W
Agentless Asset
MAC: F5 AB 8B 65 00 D4

Francois Didier
Consultant
HQ—Strategy
Remote Access
6 p.m.

Identity Information

Group:
Full-Time Employee

Group:
Contractor

Group:
Guest

+

Other Conditions

Time and Date

Posture

Location

Device Type

Access Type

Authorization
(Controlling Access)

- Broad Access
- Limited Access
- Guest/Internet
- Quarantine
- Deny Access

Access Compliance Reporting

© 2010 Cisco and/or its affiliates. All rights reserved.

Access Policy: Guest Access

Provision: Guest accounts via sponsor portal

Manage: Sponsor privileges, guest accounts and policies, guest portal

Notify: Guests of account details by print, email, or SMS

Report: On all aspects of guest accounts

© 2010 Cisco and/or its affiliates. All rights reserved.

Access Policy: Non-Authenticating Devices

NAC Profiler

Device Identification

- Determine device type
- Centralized device discovery and inventory
- Uses network device tables and analyzes endpoint traffic

Control and Audit

- Authorize based on device role
- Monitor and audit to prevent spoofing

Name	Category	Description	Active Rule(s)	LDAP	Max CF
IP Phone	Special Purpose	Based on DHCP Vendor & CDP Platform	No	Yes	40.5%
Linksys Video Cam 2	Special Purpose	Based on DHCP host name only	No	No	45%
SCADA Systems	Special Purpose	Devices with MODBUS port open	Yes	No	49.375%
Rogue Detection JP	Exceptions	Adv XML Rule: Multi MAC Vendors	No	No	50%
Hewlett-Packard JetDirect Printer	Special Purpose	Based on DHCP Vendor and/or OpenPort	Yes	No	51%
Linksys Video Cam	Uncategorized	Security Cameras	No	Yes	51%
Multi Server	GP Endpoints	Based on server banners	Yes	No	85.56%
Apple Users	GP Endpoints	Based on User Agent	No	No	92%
Windows Users	GP Endpoints	Based on User Agent and/or DHCP Vendor	No	No	96.925%

Many endpoint devices are undocumented and cannot authenticate to the network

IP Cameras

Alarm Systems

Fax Machines

Turnstiles

Cash Registers

HVAC Systems

Video Conference

Printers

Enterprises without VoIP Wired Endpoints Distribution

Enterprises with VoIP Wired Endpoints Distribution

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco TrustSec Portfolio

Appliance Policy Components

NAC Manager
Admin, Reporting, and Policy Store

NAC Server
Posture, Services, and Enforcement

OR

ACS
Identity & 802.1x Access Policy System

+

NAC Profiler
Profiles Non-Authenticating Devices

NAC Guest
Full-Featured Guest Provisioning Server

Endpoint Components (Optional)

NAC Agent

Web Agent

No-Cost Persistent & Temporal Clients for Authentication, Posture, & Remediation

OR

802.1x Supplicant
CSSC or OS-Embedded Supplicant

Cisco 2900/3560/3700/4500/6500 and Nexus 7000 switches, Adaptive Security Appliance (ASA), Wireless and Routing Infrastructure

© 2010 Cisco and/or its affiliates. All rights reserved.

SGT and SGACL Enforcement

For Your Reference

Unique 16 bit (65K) tag assigned to **unique role**

Represents **privilege of the source user, device, or entity**

Tagged at ingress of TrustSec domain

Filtered (SGACL) at egress of TrustSec domain

No IP address required in ACE (IP address is bound to SGT)

Policy (ACL) is **distributed from central policy server (ACS)** or configured locally on TrustSec device

Benefits

- Provides **topology-independent** policy
- Flexible and scalable policy based on user role
- **Centralized policy management** for dynamic policy provisioning
- Egress filtering **results to reduce TCAM impact**

© 2010 Cisco and/or its affiliates. All rights reserved.

How SGACL Simplifies Access Control

© 2010 Cisco and/or its affiliates. All rights reserved.

TrustSec

Cisco's End-to-End Portfolio Highlights

TrustSec Client

- Robust Feature Support
- Advanced VPN/FIPS
- Flexible Profile and Credential Support
- Seamless XML Provisioning
- NAC Agent
- Cisco SSC

IPT Integration

- Multi-Domain Auth (MDA)
- CDP Enhancement with 2nd Port Disconnect (Linkstate awareness)
- 802.1X - EAP-TLS w/ MIC or LSC

Campus Access

- Monitor Mode, Low-Impact Mode, High Security Mode for flexible roll out
- Ease of deployment with Flexible Auth: One configuration fits all
- Secure Group Tagging

Policy Servers

- **AAA RADIUS**
  - Cisco ACS 5.1
- **Wired Guest Access Solution**
  - NAC Guest Server
- **Profiling**
  - NAC Profiler
- **Posture**
  - NAC Appliance

Business Value

- Solution Expertise
- Reduced Vendor Support
- Cisco Stability
- Reduced operational cost

A.11 Access control

For Your Reference

- A.11.2 User Access Management

  Objective: to ensure authorized user access and to prevent unauthorized access to information systems.

  A.11.2.3 User password management

  –Active Directory (AD), CLI, and ACS/ISE

  A.11.2.4 Review of user access rights

  –Active Directory (AD), and ACS/ISE

© 2010 Cisco and/or its affiliates. All rights reserved.

Password Security

- password: sets a password for a line and user EXEC mode
- username password: sets a password for a local username
- enable password: sets a local password to restrict access to the various EXEC mode privilege levels. By default, password is stored in clear text
- enable secret: sets a local router password for EXEC privilege levels and stores the password using a nonreversible cryptographic hash function
- service password-encryption: encrypts all local passwords including line, username, enable, and authentication key passwords
  - Useful if an unauthorized user obtains a copy of your configuration file
  - It should be noted that this command invokes the same Type 7 encryption algorithm used by the enable password CLI

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.3 User Responsibilities

  Objective: to prevent unauthorized user access, and compromise or theft of information and information processing facilities

  A.11.3.1 Password use

  –Active Directory (AD)

  A.11.3.2 Unattended user equipment

  –Screensaver

  –Network devices timeout

  A.11.3.3 Clear desk and clear screen policy

  - Cisco Secure Desktop (CSD)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.1 Policy on use of network services

  – Cisco ACS /ISE

  – Cisco NAC /ISE

  – Cisco ASA

  –.1x

  –Cisco TrustSec

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco NAC Components

Policy

NAC Manager
Centralized management, configuration, reporting, and policy store

Ruleset Updates
Scheduled automatic rulesets for anti-virus, Microsoft hot-fixes and other applications

ACS
RADIUS-based access policy for 802.1X termination

Services

NAC Server
Posture, services and enforcement

NAC Guest
Full-featured guest provisioning server

NAC Profiler
Aggregates data from Collector to determine role and privileges

NAC Collector
Collects network data to determine device type

NADs

ASA VPN

Wireless

Switch

Endpoints

NAC Agent or Web Agent
No-cost client for device-based scans.

802.1X Supplicant
802.1X supplicant via CSSC or native OS

© 2010 Cisco and/or its affiliates. All rights reserved.

Functions Map to Solution Components

Identity + Posture

RBAC, Device Compliance, Threat Containment

NAC Manager

NAC Server

NAC Agent

Guest Lifecycle Management

Increased Productivity, Operational Efficiency

NAC Guest Server

Device Profiling & Provisioning + Behavior Monitoring

Inventory Management, Operation Efficiency

NAC Profiler

NAC Collector

Standalone appliance or licensed as a module on NAC Server

© 2010 Cisco and/or its affiliates. All rights reserved.

NAC Automated Ruleset Updates

Cisco NAC Manager

AutoUpdates
Hotfixes
Service Packs
Windows Updates

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.2 User authentication for external connections

  – Cisco VPN Solutions

  – Cisco ACS/ISE

  – Cisco ASA

  – Cisco IOS firewall on the ISR

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.3 Equipment identification in network

  – Cisco NAC profiler /ISE

  –Cisco TrustSec (Device Access Control)

  –Cisco CleanAir for Wireless

  –SNMP

© 2010 Cisco and/or its affiliates. All rights reserved.

CleanAir Technology

Integrated spectrum intelligence

- Detects, classifies, locates and mitigates RF interference
- Self-heals and optimizes wireless performance
- Purpose-built radio chipset for spectrum intelligence, not software based
- Cisco Aironet 3500 Series Access Points
- Secures against non Wi-Fi threats and enforces policy automatically

"This capability has been at the top of my wish list for spectral-assurance tools since... The potential benefits in performance, reliability, security, integrity, and risk management (regulatory and related) are enormous."

– Craig Mathias, Farpoint Group

"The integration of spectrum analysis and building this intelligence into the infrastructure itself is a significant game changer… A self-healing WLAN able to work around the various sources of interference is fast becoming a requirement…"

– Mike Brandenburg, Network Computing

© 2010 Cisco and/or its affiliates. All rights reserved.

SNMP (Simple Network Management Protocol)

For Your Reference

- Canonical method of obtaining real time information from network devices
- SNMP Version 3 (SNMPv3) provides authentication, encryption
- MIBs support polling of statistics ranging from interface bandwidth to CPU utilization to chassis temperature
- Both a pull model for statistical polling and a push model for trap generation based on events such as link up/down
- Many open-source and commercial collection systems, visualization tools
- Easiest way to get into profiling of general network characteristics

© 2010 Cisco and/or its affiliates. All rights reserved.

SNMP—NMS

For Your Reference

- Network Management Systems (NMS) can serve as SNMP consoles, among other things
- Many NMS can use SNMP traps and/or other forms of telemetry as triggers for paging, scripted actions, etc.
- Pulling information together can be useful for Network Operations Centers, operations teams
- Commercial systems such as HP OpenView, Micromuse NetCool, IBM Tivoli, CA Unicenter
- Several open source systems—Big Brother (http://bb4.com/), Big Sister (http://www.bigsister.ch/), Nagios (http://www.nagios.org/), and others

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.4 Remote diagnostic and configuration port protection

  – CiscoWorks

  – ACL

  – Cisco ACS /ISE

  –Cisco Physical Security (Access Control, Cameras, Video surveillance)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.5 Segregation in networks

  –VLANs

  –DMZ

  –MPLS

  – Cisco ASA and virtual firewalls

  – Cisco Nexus and virtualization portfolio

  – VSG (Virtual Security Gateway)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.6 Network connection controls

  – Cisco ASA

  – Cisco ACS /ISE

  – Cisco VPN solutions

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.4 Network Access Control

  Objective: to prevent unauthorized access to networked services

  A.11.4.7 Network routing control

  – Cisco ASA

  – Cisco ISR

  – ACL from routing point of view, routing authentication

© 2010 Cisco and/or its affiliates. All rights reserved.

Secure Routing—Route Authentication

Configure Routing Authentication

Certifies Authenticity of Neighbor and Integrity of Route Updates

© 2010 Cisco and/or its affiliates. All rights reserved.

MD5 Neighbor Authentication

- A variety of Cisco IOS protocols support MD5 authentication including BGP, OSPF, LDP, RIPv2, IS-IS, HSRP, EIGRP, and MSDP

© 2010 Cisco and/or its affiliates. All rights reserved.

Auto Secure

- CLI command that automates the configuration of security features and disables certain features enabled by default that could be exploited for security holes

```
Router#auto secure [management | forwarding] [no-interact |
full] [ntp | login | ssh | firewall | tcp-intercept]
```

- Implements a number of best practices to help secure the router
- Released in Cisco IOS Software Releases12.3(1) mainline, 12.3T, and 12.2(18)S

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper09186a00801dbf61.html

© 2010 Cisco and/or its affiliates. All rights reserved.

Auto Secure

Auto Secure Options

- Management–Secures only Management Plane
- Forwarding–Secure only Forwarding Plane
- No-interact–No interactive configurations
- Full–Full interactive session (Default)
- NTP–Secures only NTP
- Login–Secures only Device login
- SSH–Enables SSH
- Firewall–Enables Cisco IOS Firewall
- TCP-intercept–Enables tcp-intercept

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.5 Operating system access control

  Objective: to prevent unauthorized access to operating systems

  A.11.5.1 Secure log-on procedures

  ACS and AD, single sign on (SSO), router access tools

  A.11.5.2 User identification and authentication

  –ACS and AD, single sign on (SSO), router access tools,

  –Access Control on ASA firewall

  –Appilcation access control on ASA firewall

© 2010 Cisco and/or its affiliates. All rights reserved.

Access to the Router

- Console and VTY
- SSH—encrypted access
- Telnet (prefer SSH)
- Local passwords
  - Usernames configured on the router with
- External AAA
  - TACACS+, RADIUS, Kerberos
- One-time passwords (OTP)
- HTTP/HTTPS
- SNMP

© 2010 Cisco and/or its affiliates. All rights reserved.

Limit Authority—Authorize Commands

- Differentiate staff authority on the router
  - Help desk
  - Operations
  - Second-level/third-level support
- Use privilege levels (0–15)

© 2010 Cisco and/or its affiliates. All rights reserved.

Set Privileges

- Set level of privilege for each user class

```
privilege exec level 5 show ip route
privilege exec level 5 configure terminal
privilege exec level 5 show version
privilege configure level 5 interface
privilege interface level 5 shutdown
```

- Initially difficult to deploy
- Long-term benefit outweighs short-term pain

© 2010 Cisco and/or its affiliates. All rights reserved.

Access Control on Cisco ASA

Comprehensive, Granular Controls

- Flexible, granular controls
- Application and user-centric security
- Acceptable use management

© 2010 Cisco and/or its affiliates. All rights reserved.

Application and User-Centric Security for ASA

Access Control for Modern Networks

Application Access Control

- Integrated HTTP & Port 80
- IM & P2P
- Content type & Active-X

Authentication Policies

- Selective access to assets
- Track and audit user activity
- Extensive protocol support

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.5 Operating system access control

  Objective: to prevent unauthorized access to operating systems

  A.11.5.3 Password management system

  – Cisco ACS (and AD)

  A.11.5.4 Use of system utilities

  – Cisco ACS (authentication and authorization)

  –IBM Tivoli and HP OpenView

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.5 Operating system access control

  Objective: to prevent unauthorized access to operating systems

  A.11.5.5 Session time-out

  –IOS timeout features, VPN timeout, etc

  A.11.5.6 Limitation of connection time

  –IOS commands timeout: ssh, telnet, etc

© 2010 Cisco and/or its affiliates. All rights reserved.

Disable Idle User Sessions

- To mitigate the risk associated with idle user sessions:

  exec-timeout: disconnects incoming user sessions after a specific period of idle time

  ip http timeout-policy idle: disconnects idle HTTP (or HTTPS) client connections after a specific period of idle time

- To verify whether a remote host associated with a previously connected TCP session is still active and reachable:

  service tcp-keepalives-in: to generate keepalive packets on inactive incoming network connections (initiated by the remote host)

  service tcp-keepalives-out: to generate keepalive packets on inactive outgoing network connections (initiated by a local user)

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

For Your Reference

- A.11.6 Application and information access control

  Objective: to prevent unauthorized access to information held in application systems

  A.11.6.1 Information access restriction

  – Cisco TrustSec

  –Cisco NAC

  –ACLs

  –DAP (Dynamic Access Policy)

  – Cisco SSL VPN

  – Cisco IPS

  – Cisco ACS

  A.11.6.2 Sensitive system isolation

  –Zoning, VLANs, Virtualization, MPLS VRF, VMWare, VSG

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.7 Mobile Computing and Teleworking

  Objective: to ensure information security when using mobile computing and teleworking facilities

  A.11.7.1 Mobile computing and communications

  – Cisco AnyConnect

  – Cisco VPN SSL

  – Cisco VPN IPSec

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco AnyConnect Secure Mobility

Web Security with Next Generation Remote Access

Choice

Diverse Endpoint Support for Greater Flexibility

Security

Rich, Granular Security Integrated Into the network

Experience

Always-on Intelligent Connection for Seamless Experience and Performance

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco AnyConnect VPN Client

Secure Network Access

Cisco AnyConnect Essentials

- Automatically downloadable
- Access to almost any application or resource
- Automatic updates
- Robust, easy connections
- Optimized for mobile users
- IPv4 and IPv6 network access
- Voice friendly (DTLS)

Cisco AnyConnect Premium

Enhances AnyConnect Essentials features

- Clientless SSL support
- Cisco Secure Desktop Vault for secure access from unmanaged endpoints
- Cisco Secure Desktop Host Scan for pre-connect posture checks

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco AnyConnect Mobile
Tunneling (Microsoft Windows Mobile)

For Your Reference

- Microsoft Windows Mobile 6.1, 6.0, and 5.0
- Touch-screen devices
- Secure remote access to enterprise applications from Microsoft Windows Mobile

© 2010 Cisco and/or its affiliates. All rights reserved.

Apple iPhone VPN
Tunneling (Apple iPhone)

For Your Reference

- Apple iPhone and iPod touch compatible
- Secure remote access to enterprise applications
- IPsec VPN tunneling
- No unique configuration required on head-end side

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco AnyConnect Secure Mobility

A Next Generation Solution

1 AnyConnect
Secure Mobility Client

- Simplified remote access
- Connection and app persistence
- Always-on VPN enforcement

2 Web Security Appliance
Richer Web Controls

- Location-aware policy
- Application controls
- SaaS Access Control

3 Combined Solution
End-to-End Seamless Security

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco AnyConnect Secure Mobility Client

- More Intelligence
  - Optimal Gateway Detection
  - Trusted Network Detection
- More Security
  - Always-On VPN administrative control
  - Quarantine capability
- Better User Experience
  - Hotspot/Captive Portal detection
  - Local print access

© 2010 Cisco and/or its affiliates. All rights reserved.

Extending Security and Control to SaaS

Identity Integration with SAML Enabled Gateway

- **Usability**: Sign into SaaS applications using same AD credentials
- **Security**: Zero-day revocation of SaaS permissions
- **Simplicity:** Integrated SAML Identity Provider

© 2010 Cisco and/or its affiliates. All rights reserved.

A.11 Access control

- A.11.7 Mobile Computing and Teleworking

  Objective: to ensure information security when using mobile computing and teleworking facilities

  A.11.7.2 Teleworking

  –Cisco AnyConnect

  –CVO (Cisco virtual office)

  –VPN (SSL, IPSec)

  – Cisco NAC /ISE

© 2010 Cisco and/or its affiliates. All rights reserved.

What is “The Virtual Office?”

ANYWHERE

- Single phone line
- Single wireless network
- Same secure application and resource access

© 2010 Cisco and/or its affiliates. All rights reserved.

CVO Teleworker Solution

Bringing office-caliber resources to remote employees

© 2010 Cisco and/or its affiliates. All rights reserved.

CVO Technologies

For Your Reference

Remote Site

Cisco 800 Series Secure Wireless Integrated Router

Cisco Unified Phone 7900 Series

Head-End

Cisco Secure Router with VPN

Configuration Engine for Touch Free Deployment

© 2010 Cisco and/or its affiliates. All rights reserved.

CVO Deployment Models

For Your Reference

Cisco Virtual Office

(larger deployments)

Full featured management infrastructure includes services for policy definition, identity, and automated configuration push

Cisco Virtual Office Express

Simplified single device head-end infrastructure for fastest setup and deployment

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Virtual Office Use Cases

For Your Reference

HOME OFFICE

- Part/Full-Time Telecommuter
- Shared Connection

SMALL BRANCH

- Fixed Location
- More Than One User

CALL CENTER

- Fixed or home office
- Convenient Services

MOBILE USER

- Fixed or home office
- Convenient Services

© 2010 Cisco and/or its affiliates. All rights reserved.

CVO benefits vs. VPN

For Your Reference

- Seamless experience Office vs. Home with CVO
- Additional support for content-rich applications (Web 2.0)
- Comprehensive QoS for optimal voice and video
- Available Unified Wireless
- Layered Security supported: PKI, Firewall, IPS, NAC, port-security 802.1x, and Content Filtering

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Connectivity Solution

The Virtual Office Solution for Teleworkers

For Your Reference

Extend Trusted Network to Home and Branch Offices with CVO and ISR

AnyConnect Secure Mobility Client

Purpose-Optimized Head Ends: ASA and IOS VPN

CVO = Cisco Virtual Office

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

For Your Reference

- A.12.1 Security requirements of information systems

  Objective: to ensure that security is an integral part of information systems

  A.12.1.1 Security requirements analysis and specification

  –Cisco Services

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

- A.12.2 Correct processing in applications

  Objective: to prevent errors, loss, unauthorized modification or misuse of information in applications

  A.12.2.1 Input data validation

  –Cisco IPS

  – Cisco ASA application inspection

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Application Inspection and Control on ASA

Protocol Depth and Breadth

HTTP

- Do not allow credit card numbers in the clear.
- Impose maximum URL length

Instant Messaging/ P2P

- **Block Kazaa P2P**
- **Do not allow IM file transfer or whiteboard.**

SIP/H.323/ SCCP

- Prevent Gaming applications embedded in SIP

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Application Inspection and Control on ASA

Protocol Depth and Breadth

DNS

- **Enforce legitimate zone transfers, private versus public domains**
- **DNS spoofing and cache poisoning prevention**

SMTP/ ESMTP

- **Block *.exe attachments.**
- **E-mail only to or from my domain.**

FTP

- **Prevent tree traversal**
- **Allow limited set of verbs**

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

- A.12.2 Correct processing in applications

  Objective: to prevent errors, loss, unauthorized modification or misuse of information in applications

  A.12.2.2 Control of internal processing

  A.12.2.3 Message integrity

  –VPN - MACing (Message Authentication Code) – hashing

  –ESA email encryption

© 2010 Cisco and/or its affiliates. All rights reserved.

IronPort Encryption

Easy for the Sender…

- Automated key management
- No desktop software requirements
- Send to any email address seamlessly

© 2010 Cisco and/or its affiliates. All rights reserved.

IronPort Encryption

Easy for the Recipient...

1. Open Attachment

2. Enter password

3. View message

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

For Your Reference

- A.12.2 Correct processing in applications

  Objective: to prevent errors, loss, unauthorized modification or misuse of information in applications

  A.12.2.4 Output data validation

  –MACing

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

- A.12.3 Cryptographic controls

  Objective: to protect confidentiality, authenticity, or integrity of information by cryptographic means.

  A.12.3.1 Policy on the use of cryptographic controls

  –VPN (SSL, IPSec, DMVPN, GET VPN)

  –ISR G2

  –ASA

  –Secure Wireless

  –IP Communication (video, audio, broadcast) - encrypted voice and control signaling (ASA)

  – Cisco TrustSec 802.1 AE-based Encryption for date integrity and confidenitality (MacSec)

© 2010 Cisco and/or its affiliates. All rights reserved.

Confidentiality and Integrity 802.1AE-based Encryption

- Provides strong 128-bit AES-GCM* encryption (NIST** Approved)
- Line-rate encryption / decryption
- Standards-based key management: IEEE802.1X-REV

802.1AE

Benefits

- Protects against man-in-the-middle attacks (snooping, tampering, replay)
- Network service amenable to hop-by-hop approach compared to end-to-end approach (e.g., IPsec enforcement)

* NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

* Galois/Counter Mode

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco TrustSec Technology:
Next-Generation Security

Clear Data and Video Streams in LAN

Encrypted, Tamper-Proof Transactions

Malicious Guest User

Is My Network Ready for Current and Future Regulatory Requirements?

© 2010 Cisco and/or its affiliates. All rights reserved.

802.1AE (MACSec) and 802.1X-REV (MKA)

1. User bob connects.
2. Bob's policy indicates endpoint must encrypt.
3. Key exchange using MKA, 802.1AE encryption complete.
   User is placed in corporate VLAN.
   Session is secured.
4. User steve connects
5. Steve's policy indicates endpoint must encrypt.
6. Endpoint is not MACSec enabled.
   Assigned to guest VLAN.

802.1X-Rev Components

- MACSec enabled switches
- AAA server 802.1X-Rev aware
- Supplicant supporting MKA and 802.1AE encryption

© 2010 Cisco and/or its affiliates. All rights reserved.

MacSec Access Port (Crypto)

For Your Reference

- Standards-based encryption on user ports (IEEE 802.1AE)
  - Announcing on new Cat 3K first
- MacSec Key Agreement (MKA) standards-based key exchange protocol (IEEE 802.1X-REV MACSec Key Agreement)
- Some newer Intel LOM chip sets support MacSec
- MACSec-ready hardware:
  - Intel 82576 Gigabit Ethernet Controller
  - Intel 82599 10 Gigabit Ethernet Controller
  - Intel ICH10 - Q45 Express Chipset (1Gbe LOM)
    (Dell, Lenova, Fujitsu, and HP have desktops shipping with this LOM.)

© 2010 Cisco and/or its affiliates. All rights reserved.

Inter Data Center Encryption – MACSEC (802.1AE) over EoMPLS

For Your Reference

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Wireless Security Overview

Integrated

Built into the wireless infrastructure

WIPS

Access Control

Auth/Privacy

Clean RF

Management & Reporting

Proactive

Hardened wireless core to prevent attacks before they happen

Infrastructure Authentication

MFP

Automated Vulnerability Monitoring

Collaborative

Wired and wireless network security working together

Malware Mitigation

Posture Assessment

Unified Security Management

Cisco Borderless Network Architecture

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco ASA Phone Proxy

Remote Access and Voice/Data Segmentation

- Leverage native Cisco IP Phone encryption (TLS/SRTP) to enable secure calls from IP Phones on un-trusted, remote networks
- Seamless deployment and operation with minimal impact on existing UC infrastructure
- Simplified user experience – Plug and play
- A Remote Access UC Solution for UC devices

© 2010 Cisco and/or its affiliates. All rights reserved.

Industry-First Encrypted Voice Security Solution

Any Cisco voice/video communications encrypted with SRTP/TLS can now be inspected by Cisco ASA 5500 Adaptive Security Appliances:

- Maintains integrity and confidentiality of call while enforcing security policy through advanced SIP/SCCP firewall services
- TLS signaling is terminated and inspected, then re-encrypted for connection to destination (leveraging integrated hardware encryption services for scalable performance)
- Dynamic port is opened for SRTP encrypted media stream, and automatically closed when call ends

© 2010 Cisco and/or its affiliates. All rights reserved.

VPN Technology Positioning

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

- A.12.3 Cryptographic controls

  Objective: to protect confidentiality, authenticity, or integrity of information by cryptographic means.

  A.12.3.2 Key management

  –GET VPN

  –Key server management

  –Certificate Authority

© 2010 Cisco and/or its affiliates. All rights reserved.

Group Security Functions

© 2010 Cisco and/or its affiliates. All rights reserved.

Group Security Elements

For Your Reference

© 2010 Cisco and/or its affiliates. All rights reserved.

Basic GET VPN Architecture

For Your Reference

- Step 1: Group Members (GM) “register” via GDOI with the Key Server (KS)
  - KS authenticates & authorizes the GM
  - KS returns a set of IPsec SAs for the GM to use

© 2010 Cisco and/or its affiliates. All rights reserved.

Basic GET VPN Architecture

For Your Reference

- Step 2: Data Plane Encryption
  - GM exchange encrypted traffic using the group keys
  - The traffic uses IPSec Tunnel Mode with “address preservation”

© 2010 Cisco and/or its affiliates. All rights reserved.

Basic GET VPN Architecture

For Your Reference

- Step 3: Periodic Rekey of Keys

  KS pushes out replacement IPsec keys before current IPsec keys expire. This is called a “rekey”

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

For Your Reference

- A.12.4 Security of system files

  Objective: to ensure the security of system files

  A.12.4.1 Control of operational software

  –IPT phone image control

  A.12.4.2 Protection of system test data

  A.12.4.3 Access control to program source code

  –IronPort

© 2010 Cisco and/or its affiliates. All rights reserved.

A.12 Information Systems Acquisition, Development and Maintenance

For Your Reference

- A.12.5 Security in Development and Support Processes

  Objective: to maintain the security of application system software and information

  A.12.5.1 Change controls procedures

  A.12.5.2 Technical review of applications after operating system changes

  A.12.5.3 Restrictions on changes to software packages

  A.12.5.4 Information leakage

  – DLP on ESA and WSA (IronPort)

  – DLP on Cisco AnyConnect

  A.12.5.5 Outsourced software development

  –Cisco Services

© 2010 Cisco and/or its affiliates. All rights reserved.

For Your Reference

A.12 Information Systems Acquisition, Development and Maintenance (Cont'd)

- A.12.6 Technical Vulnerability Management

  Objective: to reduce risks resulting from exploitation of published technical vulnerabilities.

  A.12.6.1 Control of technical vulnerabilities

  –Cisco Security Manager (CSM) / Cisco Prime

  –Cisco SPA service

  –Qualys

  –Red Seal

© 2010 Cisco and/or its affiliates. All rights reserved.

A.13 Information Security Incident Management

For Your Reference

- A.13.1 Reporting Information Security Events and Weaknesses

  Objective: to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken

  A.13.1.1 Reporting information security events

  –CSM / Prime

  – Cisco IPS

  A.13.1.2 Reporting security weaknesses

  –Cisco Advanced Services (Pen Test and Vulnerability Assessment)

  –Qualys

  –RedSeal

© 2010 Cisco and/or its affiliates. All rights reserved.

A.13 Information Security Incident Management

- A.13.2 Management of Information Security Incidents and Improvement

  Objective: to ensure a consistent and effective approach is applied to the management of information security incidents

  A.13.2.1 Responsibilities and procedures

  A.13.2.2 Learning from information security incidents

  A.13.2.3 Collection of evidence

  –Netflow - Routers (ISR), Switches, and other Cisco devices

  – Cisco ASA (logs)

  – Cisco IPS

  – Cisco ACS (AAA)

© 2010 Cisco and/or its affiliates. All rights reserved.

NetFlow - Key Concept

- Packet capture is like a wiretap
- NetFlow is like a phone bill
- This level of granularity allows NetFlow to scale for very large amounts of traffic

  We can learn a lot from studying the phone bill!

  Who's talking to whom, over what protocols and ports, for how long, at what speed, for what duration, etc.

  NetFlow is a form of telemetry pushed from the routers/switches — each one can be a sensor

© 2010 Cisco and/or its affiliates. All rights reserved.

NetFlow
Internal Threat Information Resource

```
router (config-if)# ip flow ingress
router (config)# ip flow-export destination 172.17.246.225 9996
```

- NetFlow is available on routers and switches
- Have syslog-like information without having to buy a firewall
- One NetFlow packet has information about multiple flows

NetFlow Cache

© 2010 Cisco and/or its affiliates. All rights reserved.

NetFlow—Output

Internal Threat Information Resource

```
Router#sh ip cache flow
IP packet size distribution (20286187 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .008 .038 .414 .288 .053 .005 .005 .004 .002 .010 .002 .003 .002 .005 .003

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .006 .002 .001 .053 .084 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  17 active, 4079 inactive, 3241278 added
  63971700 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol          Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------          Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          145       0.0        55    40      0.0      12.1       1.0
TCP-FTP              93       0.0         7    56      0.0       3.6       6.5
TCP-FTPD             13       0.0         3   170      0.0       2.7       4.6
TCP-WWW           74816       0.0        14   700      0.8       2.0       5.9
TCP-SMTP              9       0.0         1    51      0.0       2.7      15.4
TCP-X                90       0.0         1    40      0.0       0.0      15.5
TCP-other        107374       0.0         2   126      0.2       5.4      15.2
UDP-DNS           78837       0.0         1    63      0.0       0.4      15.4
UDP-Frag            346       0.0        60   429      0.0       4.9      15.4
UDP-other       2978205       2.4         6   216     15.4       0.6      15.4
ICMP               1280       0.0         2    67      0.0       2.5      15.5
Total:          3241208       2.6         6   240     16.7       0.8      15.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
BV1           0.0.0.0         Null          255.255.255.255 11 0044 0043     2
BV1           20.20.20.3      Null          202.123.240.34  11 13C4 13C4     1
BV1           20.20.20.3      Null          171.68.222.150  11 04C0 0405     1
BV1           20.20.20.3      Null          171.70.156.234  11 04C0 0405     1
Vi1           206.13.28.12    Local         69.108.216.109  11 0035 078E     6
BV1           20.20.20.3      Local         20.20.20.1      06 04BC 0017    56
BV1           20.20.20.3      Local         20.20.20.1      06 0499 0017    77
```

Traffic classification

Flow Summary

Detail

© 2010 Cisco and/or its affiliates. All rights reserved.

Network Behavioral Analysis (NBA)

- Networks and network enabled devices constantly create traffic. However, this traffic follows certain patterns according to the applications and user behaviour
- Analyzing these patterns allows us to see what is NOT normal
- The key is to collect traffic information (Netflow) and calculate various statistics. These are then compared against a baseline and abnormalities are then analyzed in more detail.

© 2010 Cisco and/or its affiliates. All rights reserved.

NetFlow

For Your Reference

- Cisco NetFlow home

  http://www.cisco.com/en/US/tech/tk812/tsd_technology_support_protocol_home.html

- Linux NetFlow reports HOWTO

  http://www.dynamicnetworks.us/netflow/netflow-howto.html

© 2010 Cisco and/or its affiliates. All rights reserved.

A.14 Business Continuity Management

For Your Reference

- A.14.1 Information Security Aspects of Business Continuity Management

  Objective: to counteract interruptions to business activities and to protect critical business processes from the effect of major failure of information systems or disasters and to ensure their timely resumption

  A.14.1.1 Including information security in the business continuity management process

  A.14.1.2 Business continuity and risk assessment

  A.14.1.3 Developing and implementing continuity plans including information security

  – Cisco Virtual Switching System (VSS)

  – High Availability and Failover features on all systems

  –Hot swappable power supplies

© 2010 Cisco and/or its affiliates. All rights reserved.

Virtual Switching System (VSS)

Virtual Switching System

Physical View

Logical View

Take TWO physical Catalyst 6500 switches, convert them into a VSS system, and you end up with ONE logical Catalyst 6500 switch...

A.14 Business Continuity Management

For Your Reference

- A.14.1 Information Security Aspects of Business Continuity Management

  Objective: to counteract interruptions to business activities and to protect critical business processes from the effect of major failure of information systems or disasters and to ensure their timely resumption

  A.14.1.4 Business continuity planning framework

  A.14.1.5 Testing, maintaining and re-assessing business continuity plans

  – Cisco Services

© 2010 Cisco and/or its affiliates. All rights reserved.

A.15 Compliance

- A.15.1 Compliance with legal requirements

  Objective: to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements

  A.15.1.2 Identification of applicable legislation

  – Cisco GRC Service

  A.15.1.2 Intellectual property rights

  –Intellectual Property DLP email ESA

  A.15.1.3 Protection of organizational records

  –DLP, HA storage, VPN -integrity, SME

  A.15.1.4 Data protection and privacy of personal information

  –Refer to Cisco solution for PCI Compliance

© 2010 Cisco and/or its affiliates. All rights reserved.

Evolution of Data Loss

Email Remains a Primary Loss Vector

Errant e-mails compromise hundreds of student IDs

Student Financial Services sends 632 registration block notifications containing students' Social Security numbers to the wrong students

Breanna Hockenbury, Cavalier Daily Staff Writer

Notifications from Student Financial Services intended for students whose registration was blocked were erroneously sent to the wrong students in emails that included others' Social Security numbers.

Student Financial Services intended to send 1,264 emails to alert students of registration blocks. Only 632 e-mai

SAIC warns of possible data breach

AP Associated Pres

By Donna Borak, AP Business Writer | July 20, 2007

WASHINGTON --Pentagon contractor SAIC Inc. may have compromised personal information about more than half a million military personnel and their relatives because it did not encrypt data

Verizon gaffe lets customer details slip

By Joris Evers
Staff Writer, CNET News.com
Published: August 25, 2006, 5:11 PM PDT

Verizon Wireless this week accidentally distributed a file with limited details on more than 5,000 customers outside the company, potentially giving identity thieves a toehold.

The Microsoft Excel spreadsheet file was e-mailed on Monday and includes names, e-mail addresses, cell phone numbers and cell phone models of 5,210 Verizon Wireless customers, going by a copy of the file obtained by CNET News.com. All of the customers have Motorola Razr phones, according to the spreadsheet.

The spreadsheet was inadvertently sent to about 1,800 people, all Verizon Wireless subscribers, according to a follow-up e-mail apologizing for the gaffe that the mobile carrier sent on Thursday. The Excel file was attached to an ad for a Bluetooth wireless headset, instead of the

Record Type Lost

© 2010 Cisco and/or its affiliates. All rights reserved.

Data Loss Prevention

Simple Set Up

- Easy “3 click” set-up using content filters
- Use pre-defined content categories or create / customize your own
- Can be applied to specific users under specific conditions

© 2010 Cisco and/or its affiliates. All rights reserved.

Data Loss Prevention Overview

Integrated Scanning

Custom Content Filters

Compliance Dictionaries

Smart Identifiers

Weighted Content Dictionaries

Attachment Scanning

© 2010 Cisco and/or its affiliates. All rights reserved.

DLP Overview, Cont.

Integrated Remediation

© 2010 Cisco and/or its affiliates. All rights reserved.

Recognizing Content for Custom Action

- Business Needs determine sensitive content
- Content can be tracked on key words

© 2010 Cisco and/or its affiliates. All rights reserved.

A.15 Compliance

- A.15.1 Compliance with legal requirements

  Objective: to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements

  A.15.1.5 Prevention of misuse of information processing facilities
  - Cisco Physical security
  - System Banners

© 2010 Cisco and/or its affiliates. All rights reserved.

System Banners

- A banner serves as a legal notice, such as "no trespassing" or a "warning" statement. A proper legal notice protects you such that it enables you to pursue legal actions against unauthorized users.
- EXEC banner: specifies a message (or EXEC banner) to be displayed when an EXEC process is created
- MOTD banner (message-of-the-day): specifies a MOTD to be displayed immediately to all user sessions and when new users first connect to the router
- Incoming banner: specifies an incoming banner to be displayed for incoming reverse Telnet sessions
- Login banner: specifies a login banner to be displayed before username and password prompts

© 2010 Cisco and/or its affiliates. All rights reserved.

System Banners

For Your Reference

```
banner login ^
  Authorised access only
  This system is the property of Galactic Internet
  Disconnect IMMEDIATELY if you are not an authorised user!
  Contact noc@isp.net 555-1212 for help.
^

banner motd ^
  Notice: all routers in $(domain) will be upgraded beginning July 1
^

banner exec ^
  PLEASE NOTE - THIS ROUTER SHOULD NOT HAVE A DEFAULT ROUTE!
  It is used to connect paying peers.  These 'customers' should not be able to
  default to us.  The config for this router is NON-STANDARD
  Contact Network Engineering 555-1212 for more info.
^
```

© 2010 Cisco and/or its affiliates. All rights reserved.

A.15 Compliance

For Your Reference

- A.15.1 Compliance with legal requirements

  Objective: to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements

  A.15.1.6 Regulation of cryptographic controls
  - Export license for K9
  - Written Assurance

© 2010 Cisco and/or its affiliates. All rights reserved.

A.15 Compliance

For Your Reference

- A.15.2 Compliance with Security Policies and Procedures, and Technical Compliance

  Objective: to ensure compliance of systems with organizational security policies and standards.

  A.15.2.1 Compliance with security policies and procedures

  A.15.2.2 Technical compliance checking

  –Security assessment tools

© 2010 Cisco and/or its affiliates. All rights reserved.

A.15 Compliance

For Your Reference

- A.15.3 Information Systems Audit Considerations

  Objective: to maximize the effectiveness of and to minimize interferences to/from the information systems audit process

  A.15.3.1 Information system audit controls

  A.15.3.2 Protection of information system audit tools

© 2010 Cisco and/or its affiliates. All rights reserved.

Recommendations

© 2010 Cisco and/or its affiliates. All rights reserved.

How Best to Implement Frameworks

- The best practices adopted must consider the following:
  - Tailoring
  - Aligning Best Practices with Business
    - Align IT strategy with business goals
    - Understand, define, and mitigate risks

© 2010 Cisco and/or its affiliates. All rights reserved.

How Best to Implement Frameworks

- Planning
  - Set up an organizational framework with clear responsibilities and objectives and participation from all interested parties
  - Manage risk areas
  - Analyze current capability and identify gaps
  - Develop a maturity capability assessment
  - Measure results, establish a scorecard mechanism for measuring current performance and monitor the results of new improvements

© 2010 Cisco and/or its affiliates. All rights reserved.

How Best to Implement Frameworks

- Open and Strong Support by Senior Management
  - Ideally, the top senior management should take ownership of IT governance
  - Continuous communication with senior management
  - Alignment of IT initiatives with business needs & risks
  - Performance measurement and reporting

© 2010 Cisco and/or its affiliates. All rights reserved.

How Best to Implement Frameworks

For Your Reference

- General Recommendations
  - Treat the implementation initiative as a project with phases
  - Create awareness of the business purpose and benefits of practices
  - Cultural Change
  - Manage expectations
  - Focus on quick wins
  - Framework, processes and procedures should be agile and flexible, to adapt to changes (new technologies, Org change, new demands, etc.)

© 2010 Cisco and/or its affiliates. All rights reserved.

Current and Future Considerations

© 2010 Cisco and/or its affiliates. All rights reserved.

Data Center Evolution

© 2010 Cisco and/or its affiliates. All rights reserved.

I Know How to Use “The Cloud” Already?

Request a Resource | **Pay as You Use** | **Resource Pool**

Need It –
Get It Instantly

Don’t Need it –
Give It Back

Capacity

Suitability

Performance

Green

Normalization

© 2010 Cisco and/or its affiliates. All rights reserved.

A Common Definition—Cloud Computing

IT Resources and Services that Are Abstracted from the Underlying Infrastructure and Provided On Demand" and "At Scale" in a Multitenant and Elastic Environment

A Style of Computing Where Massively Scalable IT-Enabled Capabilities Are Delivered "As a Service" to Multiple External Customers Using Internet Technologies

Source: Gartner "Defining and Describing an Emerging Phenomenon"
June 2008

Anywhere,
Anyone,
Any Service

© 2010 Cisco and/or its affiliates. All rights reserved.

Cloud-Based Services—A New Utility

Cloud Computing Is a 4th Utility
Virtualization (lower cost)
Low Complexity
Scalability
Elasticity (economies of scale)

Utility Computing and Cloud Computing Are Often Confused:

- Utility computing delivers a “pay-by-the-drink” business model in which customers receive computing resources from a service provider.
- Cloud computing relates to the way we design, build, deploy, and run applications in a virtualized environment, share resources, and dynamically grow.

© 2010 Cisco and/or its affiliates. All rights reserved.

Merging Physical to Virtual Infrastructure

© 2010 Cisco and/or its affiliates. All rights reserved.

Nexus 1000V Key Features

- Includes Key Cisco Network and Security features
- Addressing Issues for:
  - VM Isolation
  - Separation of Duties
  - VM Visibility

© 2010 Cisco and/or its affiliates. All rights reserved.

Unified Communications Threats

- Toll fraud
  - Unauthorized or unbillable resource utilization
- Eavesdropping
  - Listening to another's call
- Learning private information
  - caller ID, DTMF password/accounts, calling patterns
- Session replay
  - Replay a session, such as a bank transaction
- Fake identity
- Media tampering
- Denial of service
  - Hanging up other people's conversations
  - Contributing to other DOS attacks
- Impersonating others
- Hijacking calls
- SPAM
  - SPIM, SPIT, and more SPAM

© 2010 Cisco and/or its affiliates. All rights reserved.

Building A Secure UC System

Protecting all elements of the UC system

For Your Reference

Infrastructure

Secure connectivity and transport

Endpoints

Authenticated IP phones, soft clients and other devices

Call Control

Secure Protocols for Call Management Features

Applications

Auto-attendant, Messaging, and Customer Care

© 2010 Cisco and/or its affiliates. All rights reserved.

Secure Unified Communications
Systems Approach in Action

For Your Reference

Infrastructure
- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

Applications
- Multi-level administration
- Toll fraud protection
- Secure management
- Hardened platforms
- h.323 and SIP signaling

Call Management
- Hardened Windows OS
- Digital certificates
- Signed software images
- TLS signaling
- Integrated CSA

Endpoints
- Digital certificates
- Authenticated phones
- GARP protection
- TLS protected signaling
- SRTP media encryption
- Centralized management

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco VoIP Security Solutions

For Your Reference

Application Inspection and Control in ASA

- Application and protocol-aware inspection services provides strong application-layer security
- Performs conformance checking, state tracking, security checks, NAT/PAT support, and dynamic port allocation

H.323	MGCP	RTSP	SCCP	SIP	TAPI/JTAPI
NAT/PAT	NAT/PAT	NAT/PAT	NAT/PAT	NAT/PAT	NAT/PAT
Ver. 1–4	v0.1/v1.0	TCP	TCP	UDP/TCP	TCP
Fragmentation and Segmentation Support					

© 2010 Cisco and/or its affiliates. All rights reserved.

Voice Over Wireless LAN

Mobile voice and collaboration

- Delivers high quality voice services over the wireless LAN
- CCX enabled with intelligent QoS, fast secure roaming, and enhanced power management
- Supported on single or dual mode Wi-Fi and CCX enabled phones
- Cisco Aironet 1140, 1250, 1260 and 3500 Series Access Points
- Reduces cell phone costs and supports dual-mode applications like Cisco Mobile 8.0 for iPhone and Cisco Nokia Call Connect

"This emphasis on mobility is taking Wireless LAN technology from being a convenience to an essential part of the business environment. Cisco is describing a vision that combines WLAN voice, fixed mobile convergence, and mobile unified communications to provide the core elements for developing wireless communications-enabled business processes."

– Michael Finneran, dBrn Associates

"One of the biggest immediate benefits is for customers seeking to enable their end users to make voice calls over Wi-Fi networks and then roam on to cellular networks without losing their calls, a capability that can improve the user experience while greatly lowering calling costs."

– Matt Hamblen, Computerworld

© 2010 Cisco and/or its affiliates. All rights reserved.

Transformational World

Mobile Devices

IT Resources

- 1.3 Billion New Networked Mobile Devices in Next 3 Years

Mobility

Video

- 60% of All Cisco Network Traffic Today Is Video

10 Cisco and/or its affiliates. All rights reserved.

Changing Market Dynamics

CIO Priorities

- Acquire and retain customers
- Manage customer relationships

Lower company operating costs

–Forrester, 2008

Changing Business Demographics

- 17% branch growth by 2010
- Centralized data, distributed interactions
- By 2012–90% of consumer traffic will be video

–Nemertes, Cisco VNI, 2009

Over the Next 3 Years

- IT staff : 1.1X
- Servers: 1.8X
- Mobile users: 3X
- Information: 4.5X
- User interactions per day: 8.4X

–IDC, 2009

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Medianet

Video done right

- Offers new intelligent routing features plus architectural alternatives to guard against the risk of quality degradation due to network congestion
- Reserves resources across the entire network in order to assure a predictable and controlled Quality of Experience for each rich media session
- Reduces traffic to the Cisco WebEx cloud, optimizing the branch experience
- Performance Routing automatically routes media via the optimal route as configured by the customer

"Video Stream is a great step in the right direction…and it's only a matter of time before video becomes our primary form of communication. Cisco's strategy seems to be to drive the business by providing customers with high-bandwidth/video applications. Not a bad thing at all."

– Craig Mathias, Farpoint Group

"Medianet is the right technology at the right time on how we can offer tools to manage video."

– Nick Lippis, The Lippis Report, Podcast

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VideoStream for Wireless

Media-Ready wireless LAN

- Delivers high quality, scalable multicast video over the wireless LAN
- Prioritizes QoS for critical video content
- Scales effectively with client admission policy control
- Cisco Aironet 1140, 1250, 3500, 1260 Series Access Points
- Access point converts multicast streams to unicast

"The software update also integrates other new features to enhance the quality of experience for streaming video over wireless LAN, delivering a more 'holistic' solution than competitors do."

– Paul Debeasi, TechTarget

"Cisco announced software for its Wi-Fi products to improve video performance, reliability and scaling on 802.11n wireless networks. … VideoStream, compensates for Wi-Fi weaknesses that degrade video quality as the number of streams and clients grow."

– John Cox, Network World

© 2010 Cisco and/or its affiliates. All rights reserved.

The New Borderless Organization

Borderless Experience

Securely, Reliably, Seamlessly

© 2010 Cisco and/or its affiliates. All rights reserved.

Some Closing Thoughts

- Do not get overwhelmed
- Small steps can make a big difference
- Remember, to survive a bear attack, you don't have to be fastest person…you just need to be faster than the next guy
- Do not be the least prepared

© 2010 Cisco and/or its affiliates. All rights reserved.

Please fill the evaluation form

© 2010 Cisco and/or its affiliates. All rights reserved.

Thank you.

CISCO