CISCO WHITE PAPER

Enterprise Security Baseline for LAN, Wireless LAN, and WAN

September 2015

Table of Contents

Enterprise Security Baseline 1

Baseline Security Common to IOS and IOS-XE Devices in the LAN, WAN, and Converged Access 2

Device Management 2

Authentication Control for Device Management 3

Device Audit Capability 4

Baseline Security for the Campus Wired LAN Access 5

LAN Access Layer 5

Baseline Security for the Layer-3 LAN and Routed WAN 8

Unicast Routing Protocol 8

Multicast Routing Protocol 9

Baseline Security for the Campus Wireless LAN Controllers Using AireOS 10

Device Management 10

Authentication Control 11

Device Audit Capability 12

Additional Considerations after Enabling Baseline Security 13

Enterprise Security Baseline

The *Enterprise Security Baseline for LAN, Wireless LAN, and WAN Reference Guide* is based on the leading practices and guidance offered for design and deployment of enterprise networks, as described in the Cisco Design Zone for Enterprise at http://cisco.com/go/designzone and other guidance on http://cisco.com.

The network an organization uses has become increasingly important over time, to the point where it is often considered critical for key tasks that make an organization successful. Enterprise organizations expect their networks to function around the clock every day with minimal disruptions, and the importance of the network is expected to increase over time as it takes on additional roles supporting the Internet of Everything.

As the importance of the network increases, you must increase the resilience of the network to mitigate risks to an acceptable level. Threats to an organization's success are not just from the perspective of data theft but from the potential for disruptions to their network infrastructure. Network disruptions can have results ranging from lost revenue and severe erosion of corporate reputation to the loss of productive education time in a school. One crucial way to increase network resiliency is to increase security of the network infrastructure itself.

It can be surprising for an organization to learn that they have many abilities to increase security already existing in the network infrastructure, but that the increased security is not implemented because it is disabled by default. An organization should use those built-in features of infrastructure devices in order to enable controls that allow the network to deliver expected services without disruption, even when subjected to intentional mischief or unintentional human error.

Cisco network infrastructure elements such as Catalyst switches and Integrated Services Routers are designed with industry-leading capabilities for securing the integrity of the devices at multiple levels–from the chipset, to the firmware, to the boot-loaders and operating systems. Devices often meet many strict standards for deployment in government and payment-transaction networks. Even so, a network operator may not be aware that a choice made while configuring a device leaves a network open to unintended risks.

The enterprise security baseline described in this guide is a set of recommendations for securing an organization's network LAN, wireless LAN, and WAN, using device configurations that are relevant across most network deployments without requiring significant implementation-specific tuning. The baseline offers recommendations for basic network security based on leading practices for typical deployments, and when there are alternative choices, we describe the leading choice. We may also describe an alternative choice if it is also commonly deployed and is not significantly more challenging to implement and maintain.

The security baseline recommendations are one aspect of a defense-in-depth approach to securing your organization's network. The recommendations are grouped by use case, addressing common objectives such as device type, hierarchical network layer, and role.

This guide recommends leading practices you can use for most deployments. Organization-specific comprehensive policy and security solutions that are deployed on top of the foundation are covered outside of this guide. Some of those solutions include TrustSec, Network as a Sensor, and Network as an Enforcer.

BASELINE SECURITY COMMON TO IOS AND IOS-XE DEVICES IN THE LAN, WAN, AND CONVERGED ACCESS

Infrastructure devices such as routers and switches are targets of security attacks because of their unique role in the network. Attacking these devices can enable the ability to deny access to an organization's resources, can be used to intercept traffic, and can allow inappropriate access to privileged information—all at network-level scope.

Cisco devices running IOS and IOS-XE are shipped with less restrictive defaults than typical production enterprise network security policies allow, which allows for ease of initial setup. If the initial configuration dialog is exited immediately, many basic security features are left in their default insecure configuration. Even after going through the initial configuration dialog, there are additional steps to be used to secure these devices from unintended access and manipulation.

Cisco recommends that you secure your network devices that run IOS and IOS-XE. These guidelines assume you are using code that was released within the past few years and that already has some common service vulnerabilities disabled by default, such as **tcp-small-servers** and **udp-small-servers**. If you are running older software, you should evaluate upgrading and further examine the vulnerabilities you may need to address.

Device Management

Use the most secure options for device management:

- Disable the HTTP server for management, if your organization does not require it for identity deployments.
- Enable the secure HTTP (HTTPS) server for management, if required.
- Disable telnet for command-line access.
- Enable secure shell version 2 (SSHv2) for command line access.
- Allow command-line access originating from only management networks and use an out-of-band network interface, if possible.
- Enable secure copy (SCP) and use it exclusively for device file operations.
- Enable SNMPv3 with restricted access, if required and supported by an organization's management utilities.
- Enable SNMPv2c with restricted access, if required.

HTTPS and Secure Shell (SSH) are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) in order to provide device authentication and data encryption.

The SSH and HTTPS protocols enable secure management of the LAN device. Both protocols are encrypted for privacy, and the unencrypted protocols, Telnet and HTTP, are turned off. Enabling HTTPS automatically generates a cryptographic key to use the service. When SSH is configured after HTTPS, you do not have to explicitly generate the cryptographic key that SSH requires, unless you wish to change the default key size.

Access lists should be applied to limit command line interface (CLI) access to networks expected to source appropriate management connections.

SCP provides a secure and authenticated method for copying configuration and image files by making use of SSH as a secure transport. Enable SCP to allow secure file management with the device in order to avoid the use of less secure protocols such as TFTP and FTP.

If Simple Network Management Protocol (SNMP) is required, enable it by using SNMPv3 to authenticate and encrypt SNMP access to the devices. In the cases where SNMPv3 is not feasible for organization's management requirements, any required SNMPv2c access should be restricted to only appropriate management device networks, using infrastructure ACLs.

Example configuration

```
no ip http server
ip http secure-server
ip domain-name [domain name]
crypto key generate rsa modulus [size]
ip ssh version 2
ip scp server enable
ip access-list standard [management access list]
  permit [ip address] [mask]
line vty 0 15
  access-class [management access list] in vrf-also
snmp-server community [SNMP read-only name] ro
snmp-server community [SNMP read-write name] rw
snmp-server engineID remote [remote ip] [engine id]
snmp-server group [group] v3 priv
snmp-server user [username] [group] v3 auth md5 [password] priv aes 256 [pass-
word]
line vty 0 15
  transport input ssh
```

Authentication Control for Device Management

Recommendations for improving authentication control for device management:

- Obfuscate configuration passwords with the strongest cryptographic algorithm method available.
- Use a centralized authentication server accessible via TACACS+.
- Create local device passwords to be used only if the centralized authentication server is unavailable.

Organizations should no longer use the **enable password** or **user [user name] password** commands and instead should use the **enable secret** and **user [user name] secret** commands, which use an MD5 hashing algorithm. Additionally, passwords in the configuration file should be encrypted by default, to avoid displaying clear-text passwords, which are easily viewed by mistake.

Configure centralized user authentication by using the TACACS+ protocol to authenticate management logins on the infrastructure devices to the authentication, authorization and accounting (AAA) server. TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. Configure all management access to the network infrastructure devices (SSH and HTTPS) for control by AAA, so that network operators are easily added and removed, as your organization requires.

A local AAA user database is also defined on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Example configuration

```
username [user name] secret [user password]
enable secret [enable password]
service password-encryption
aaa new-model
tacacs server [tacacs name]
 address ipv4 [ip address]
 key [tacacs key]
aaa group server tacacs+ [tacacs group]
  server name [tacacs name]
aaa authentication login default group [tacacs group] local
aaa authorization exec default group [tacacs group] local
aaa authorization console
ip http authentication aaa
```

Device Audit Capability

Recommendations for increasing device audit capability:

- Configure a secure synchronized clock across network devices for audit logs, with the most granular measurements available.
- Archive log messages to an external syslog server.

Configure a synchronized clock by programming network devices to synchronize to at least one local network time protocol (NTP) server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configure console messages, logs, and debug output in order to provide time stamps on output, which allows cross-referencing of events in a network. If the device has a built-in hardware clock, update that clock with the time so that the most accurate times will be available during device boot events.

Output is sent to one or more syslog servers for audit. The logging level is typically set at a lower level that restricts output to only the most important messages. The logging level is set to a high debugging level only during active event investigations, in order to avoid unnecessarily taxing the device CPU.

Example configuration

```
ntp authentication-key [key number] key [ntp key]
ntp authenticate
ntp server [ip] key [key number]
ntp update-calendar
clock timezone [standard zone] [offset]
clock summer-time [summer zone] recurring
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
logging [syslog host ip]
logging trap [syslog level]
```

After configuring the baseline security for IOS and IOS-XE devices, additional security is added based on specific deployment scenarios.

BASELINE SECURITY FOR THE CAMPUS WIRED LAN ACCESS

You deploy a wired LAN using Ethernet access switches. When port counts or interconnection needs dictate, you scale at a headquarters or remote site by adding distribution switches. Typically, for simplest interconnection of three or more distribution blocks at a larger site, you add a core.

Because the campus LAN access layer is the on ramp and off ramp for an organization's users and the devices they connect to the network for their daily work, the access layer is the optimum place to introduce security policy to harden the network. This baseline security configuration is the foundation to which you can apply supplementary configuration for more comprehensive policy, access control, and segmentation.

Additional security is added outside of Layer 2 access for Layer 3 unicast and multicast services.

LAN Access Layer

Recommendations for securing the LAN access layer:

- Enable Port Security in order to protect the switch from MAC address table exhaustion.
- Enable DHCP Snooping in order to secure DHCP services from being spoofed.
- Enable Dynamic ARP Inspection in order to limit address resolution protocol (ARP) use to valid traffic.
- Enable IP Source Guard in order to prevent IP host address spoofing.
- Enable spanning-tree Bridge Protocol Data Unit (BPDU) Guard in order to protect network availability.
- Enable IPv6 Router Advertisement Guard in order to protect devices from communication with an IPv6 router connected to user access ports.
- Enable IPv6 DHCP Guard in order to protect devices from communication with an IPv6 DHCP server connected to user access ports.

Because the access layer is the connection point between network-based services and client devices, it plays an important role in protecting other users, the application resources, and the network itself from human error and malicious attacks. The access layer of the network is protected using first-hop security with Catalyst Integrated Security Features and spanning-tree configuration.

Configure Port Security in order to limit the number of MAC addresses that can be active on the interface at one time; additional MAC addresses are considered to be in violation, and their traffic will be dropped. Port Security protects the switch MAC address table resources from exhaustion, which would result in Layer 2 flooding or "hub" behavior on the switch and the potential for traffic interception for man-in-the middle attacks. Limiting the MAC addresses also protects DHCP services from a denial-of-service attack by disallowing excessive DHCP address requests to exceed the addresses available in the DHCP scope, which would result in legitimate hosts being unable to obtain an address.

The number of MAC addresses allowed on each interface for Port Security is specific to the organization. However, the popularity of virtualization applications, IP phones, and passive hubs on the desktop drives the need for the number to be larger than one. Choose a number that allows flexibility in the organization while still protecting the network infrastructure. A few addresses may be fine, and a dozen addresses per port is more than enough for most organizations and achieves the balance required to protect the infrastructure. You limit the number of packets per second that an interface needs to inspect in order to control the use of switch CPU resources.

Configure DHCP snooping globally on the access layer VLANs, which are not trusted to supply network infrastructure services. The switch intercepts and safeguards DHCP messages within the VLAN. This ensures that an unauthorized DHCP server on another user access port cannot serve up addresses to end-user devices. Unintended DHCP servers can offer unusable DHCP addresses, causing a denial of service, or these servers can supply information that can support man-in-the-middle attacks. Uplinks ports to the network infrastructure where DHCP services are located are the only ports trusted to supply DHCP information. To control the use of switch CPU resources, you limit the number of packets per second that an interface needs to inspect.

Configure dynamic ARP inspection (DAI) to inspect ARP packets and verify the information against information captured in the DHCP snooping binding table. The switch ARP cache is only updated if the ARP is validated against the known good information, and relaying of other ARP information is disallowed, denying the ability to spoof a host address and intercept traffic for man-in-the-middle attacks.

Configure IP Source Guard on the access interfaces. IP Source Guard is applied to on non-routed interfaces as a means of preventing incorrect IP addresses on the LAN, which can be used for IP host spoofing and denial-of-service attacks.

You should configure IPv6 First Hop Security because:

- Layer 2 connectivity is available between hosts in the access layer.
- Many of the latest device operating systems have IPv6 enabled by default, and it often is the preferred means of communication.

IPv6 FHS is beneficial for hosts, regardless of the use of IPv4 or IPv6 routing configuration in the rest of the routed network.

Configure IPv6 First Hop Security to intercept and drop IPv6 router advertisements from devices connected to user access ports. Blocking the advertisements mitigates intentional and unintentional denial-of-service attacks and man-in-the-middle attacks among devices connected to the access layer. Additionally, configure IPv6 First Hop Security DHCP Guard to protect devices from communication with an IPv6 DHCP server appearing on user access ports, and enabling a communications channel.

Access layer edge ports are typically configured to be in spanning-tree portfast (also known as *edge port*) mode. If a PortFast-configured interface receives a BPDU, an invalid configuration exists, such as the connection of an unauthorized device. The BPDU guard feature prevents loops by moving a non-trunking interface into an errdisable state when a BPDU is received on an interface when PortFast is enabled. BPDU guard prevents data packet looping, which can disrupt switch and network operation

Example configuration

```
ip dhcp snooping vlan [vlan]
! next line optional for some DHCP server requirements
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan [vlan]
spanning-tree portfast bpduguard default
ipv6 nd raguard policy [host policy]
  device-role host
interface range [interface type] [port number]-[port number]
  description User host access ports
  switchport port-security maximum [mac address number]
  switchport port-security
  switchport port-security aging time [minutes]
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip arp inspection limit rate [rate]
  ip dhcp snooping limit rate [rate]
  ip verify source
  ipv6 nd raguard attach-policy [host policy]
  ipv6 dhcp guard
interface [interface type] [number]
  description Uplink to network infrastructure services
  ip arp inspection trust
  ip dhcp snooping trust
```

BASELINE SECURITY FOR THE LAYER-3 LAN AND ROUTED WAN

Unicast Routing Protocol

Recommendations for securing the unicast routing protocol in the LAN and WAN:

- Enable router neighbor control by using a default passive interface configuration.
- Enable authentication to all routing neighbors.

You prevent unintended disruptions to your Layer 3 routing infrastructure by limiting neighbor relationships to trusted routing devices.

The first step in securing your routing protocol is to allow neighbor routers to communicate on only the interfaces you explicitly enable for routing. You enable this behavior by making all interfaces passive in your chosen routing protocol and then explicitly enabling any specific interfaces intended for routing relationships.

The second step is to securing your routing protocol is to authenticate the neighbor device. You configure authentication for enhanced interior gateway routing protocol (EIGRP) named mode by using global parameters, and you configure authentication for EIGRP classic (numbered) mode and open shortest path first (OSPF) by using commands on the Layer 3 interface.

Example configuration

```
key chain [chain name]
 key 1
  key-string [neighbor key]
router eigrp [name]
 address-family ipv4 unicast autonomous-system [AS number]
  af-interface default
   passive-interface
  exit-af-interface
  af-interface [interface type] [number]
   authentication mode md5
   authentication key-chain [chain name]
   no passive-interface
  exit-af-interface
 exit-address-family

key chain [chain name]
 key 1
  key-string [neighbor key]
router eigrp [number]
  passive-interface default
```

```
    no passive-interface [interface type] [number]
  interface [interface type] [number]
    description Link to neighbor EIGRP router
    ip authentication mode eigrp [number] md5
    ip authentication key-chain eigrp [number] [chain name]

  router ospf [number]
   address-family ipv4 unicast autonomous-system [AS number]
    passive-interface default
  interface [interface type] [number]
    description Link to neighbor OSPF router
    ip ospf message-digest-key 1 md5 [neighbor key]
```

Multicast Routing Protocol

Recommendations for securing the multicast routing protocol in the LAN and WAN:

- Enable protection against rogue multicast traffic sources.
- For both static rendezvous point (RP) and auto-RP configurations, enable protection controls against unintended RPs.

IP multicast routing is required in many enterprise LANs and WANs for one-to-many services such as music on hold, organization-wide video update presentations, and other streaming media applications. PIM Sparse Mode is the most common protocol used for multicast deployments in enterprise networks and requires the use of an RP. The RP is either statically configured across all routers or an auto-RP configuration is used to distribute the RP information, giving more flexibility with multicast services migration and growth in the future. Because the multicast infrastructure is designed to replicate high-bandwidth traffic efficiently and is required for some very visible uses, you should protect the multicast infrastructure against being disrupted or being used to deliver unwanted traffic.

To protect against rogue multicast sources consuming network resources, configure a standard access control list for PIM register requests to the RP, limiting multicast traffic to acceptable source IP addresses. Alternatively, use an extended ACL to limit both the source IP addresses and the multicast group addresses.

To protect against a misconfigured or maliciously configured router advertising itself and being accepted as an unintended multicast rendezvous point, you manually configure the valid RPs on every multicast router in your network, disallowing automatic RP configuration. This method of RP control has the most comprehensive restrictions.

Alternatively, to allow your RP configuration to remain flexible to change over time and to reduce manual overhead, limit RP configuration to a single dynamic method, such as auto-RP, and ignore other methods at all routers. Apply a filter to the auto-RP mapping agents in order to restrict RPs that are permitted. This method depends on valid RP mapping agents.

Both methods allow restrictions on groups permitted from an RP.

Example configuration

```
ip access-list extended [MCAST-SOURCE ACL]
  permit ip [MCAST SOURCE NET] [MASK] [MCAST GROUP] [MASK]
  deny ip any any
ip pim accept-register list [MCAST-SOURCE ACL]

ip access-list standard [STATIC-RP ACL]
  permit 224.0.1.39
  permit 224.0.1.40
  deny any
ip pim rp-address [RP IP ADDRESS] [STATIC-RP ACL] override

! Configuration additions for an auto-RP mapping agent
ip access-list standard [RP ACL]
  permit [RP NET] [MASK]
ip access-list standard [PERMITTED GROUP]
  permit [MCAST GROUP] [MASK]
  deny any
ip pim rp-announce-filter rp-list [RP ACL] group-list [PERMITTED GROUP]
! Configuration for multicast auto-RP listeners
ip pim autorp listener
ip pim accept-rp auto-rp
```

BASELINE SECURITY FOR THE CAMPUS WIRELESS LAN CONTROLLERS USING AIREOS

Wireless LAN controllers running AireOS have a number of settings to be verified or changed from the default settings.

Device Management

Recommendations for the most secure options for device management:

- Enable SSHv2 for command line access.
- Allow CLI and web access originating from only management networks.
- Enable SNMPv2c with restricted access, if required
- Enable SNMPv3 with restricted access, if required and supported by an organization’s management utilities.

Secure HTTPS and SSH are more secure replacements for the HTTP and Telnet protocols. They use SSL and TLS in order to provide device authentication and data encryption. The SSH and HTTPS protocols enable secure management of the WLAN device. SSH is used for CLI access, and HTTPS is used for GUI access. Both protocols are encrypted for privacy.

Access lists should be applied to limit CLI and web access to networks expected to source appropriate management connections.

If SNMP is required, enable it by using SNMPv3 to encrypt SNMP access to the devices. In the cases where SNMPv3 is not feasible for organization's management requirements, you should restrict any required SNMPv2c access to only appropriate management device networks, using infrastructure ACLs..

Example Configuration

During the initial controller setup, you should enable SSH for CLI configuration. After initial setup you can also use the **service sshd** command.

Using the management tab of the GUI, enable SNMPv2c or SNMPv3 and specify the communities and their permissions.

Use the GUI security tab and access control lists functions in order to apply restrictions to management access.

Authentication Control

Recommendations for improving authentication control for device management:

- Use a centralized authentication server accessible via TACACS+.
- Create local device passwords to be used only if the centralized authentication server is unavailable.

A TACACS+ server such as Cisco Secure Access Control System (ACS) is typically used for the authentication by network administrators to the wireless network infrastructure. Configure centralized user authentication by using TACACS+ to authenticate management logins on the WLAN controllers using the AAA server. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. Configure all management access to the network infrastructure devices (SSH and HTTPS) for control by AAA, so that network operators are easily added and removed, as your organization requires.

A local AAA user database is also defined on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Example Configuration

Use the GUI security tab and AAA/TACACS+ menus to configure a TACACS+ authentication server and shared secret key, as well as the local user database.

Device Audit Capability

Recommendations for increasing device audit capability:

- Configure a secure synchronized clock across network devices for audit logs, with the most granular measurements available.
- Archive log messages to an external syslog server.

Configure a synchronized clock by programming network devices to synchronize to at least one local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configure logging output to be sent to one or more syslog servers for audit.

Example Configuration

During the initial controller setup, you should enable NTP. After initial setup you can also use the **ntp** CLI commands.

You can configure syslog messaging from the command line by using the **logging** commands.

Additional Considerations after Enabling Baseline Security

Securing an organization's network requires a defense-in-depth approach. The baseline security configuration recommendations are a starting point for securing devices in ways that are appropriate for most commonly deployed LAN, WLAN, and WAN networks. There are additional device capabilities that you should investigate. They are not covered as part of the baseline because they require extensive tuning, have dependencies on less common network service availability, or are restrictive to specific device hardware capabilities that do not currently have widespread deployment.

Listed here are some examples of capabilities that you should investigate for enhanced security in your organization's deployment:

- Control Plane Policing (CoPP) and Control Plane Protection (CPPr)
- 802.1AE MACsec link encryption
- 802.1X monitor mode minimally up to a complete policy infrastructure with TrustSec
- Traffic visibility via NetFlow monitoring
- Customized Quality of Service (QoS) policy in order to prioritize traffic based on business intent
- Private VLANs, VLAN ACLs, Port-based ACLs
- SPAN/RSPAN, IPS/IDS, and NAM
- MAC address notification
- Multilevel authorization policies for device configuration

Beyond these topics, network operators should seek to continually evaluate and improve their security exposure, by monitoring security awareness sites, such as from the Cisco Product Security Incident Response Team (PSIRT) at http://www.cisco.com/go/psirt.

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, “DESIGNS”) IN THIS MANUAL ARE PRESENTED “AS IS,” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)