the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Cisco IOS Branch

Version 1.0.0
November 2011

http://cisecurity.org
feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Cisco IOS*, provides prescriptive guidance for establishing a secure configuration posture for *Cisco IOS* version *15.0M* running on *Cisco routing and switching platforms*. This guide was tested against *Cisco IOS IP Advanced Services v15.0.1* as installed by *c880data-universalk9-mz.150.1.M4.bin*. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate *Cisco IOS* on Cisco routing and switching platforms.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Justin Opatrny
Maintainers
Justin Opatrny
Chris Jackson, *Cisco Systems, Inc., CCIE #6256 SEC & R&S, CISA, GSNA, GCIH, GCIA, GCFW, CISSP, MCSE*

Editors
Steven Piliero, *Center for Internet Security*
Testers
Justin Opatrny

Contributors and Reviewers
Ahmed Adel
Ankit Agarwal, *OPNET Technologies, Inc.*
Adam Baines
Wade Blackwell
Vu Dao Quang
Dan Didier, NetSecureIA, Inc.
Blake Frantz, *Center for Internet Security*
Michael Hamelin
Chris Jackson, *Cisco Systems, Inc., CCIE #6256 SEC & R&S, CISA, GSNA, GCIH, GCIA, GCFW, CISSP, MCSE*
Ashwin Kohli
Slava Kurenyshev
Andy McConnell, *Tripwire, Inc.*
Tim Muniz, *Tenable Network Security, Inc.*
Jason Nehrboss, *Computer Sciences Corporation*
Sergev Pavlov
Vinoth Sivasubramanian
Reed Stone, Pantex
Egor Sushkov
Jeff Weekes, *Terra Verde, LLC*

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- do not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernible in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

1. Recommendations

1.1 WAN Routing Security

Description:
This section focuses on items that provide additional information and protection for dynamic routing protocols.

1.1.1 Default Passive Interface for Routing Protocols (Level 2, Scorable)

Description:
By default, routing updates go out every active interface unless specified. The passive-interface command allows the administrator to granularly restrict routing updates to only necessary interfaces.

Rationale:
An attacker can use the information generated by or destine to the interface to begin mapping the network. In addition, the attacker can attempt to inject and manipulate the routing table.

1.1.1.1 Default Passive Interface for EIGRP (Level 2, Scorable)

Description:
Do not automatically send EIGRP routing updates out any interface.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to disable all interfaces from sending and receiving routing updates by default...

```
hostname(config)# router eigrp <virtual-instance-name>
hostname(config)# passive-interface default
```

Audit:
Perform the following to determine if this is set properly:

```
hostname# sh run | beg router eigrp
```

Default Value:
Default passive-interface is not enabled by default.

References:

1. Cisco Enterprise Branch
2. Cisco IOS IP Routing: EIGRP Configuration Guide, Release 15.0

1.1.1.2 Default Passive Interface for OSPF (Level 2, Scorable)

Description:
Do not automatically send OSPF routing updates out any interface.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to disable all interfaces from sending and receiving routing updates by default...

```
hostname(config)# router ospf <ospf_process-id>
hostname(config)# passive-interface default
```

Audit:
Perform the following to determine if this is set properly:

```
hostname# sh run | beg router ospf
```

Default Value:
Default passive-interface is not enabled by default.

References:
1. Cisco Enterprise Branch
2. Cisco IOS IP Routing: OSPF Configuration Guide, Release 15.0

1.1.2 Log Neighbor Adjacency Changes (Level 2, Scorable)

Description:
Enable logging of routing neighbor changes.

Rationale:
Detection of adjacency changes is useful for troubleshooting and may indicate an attack.

1.1.2.1 Log EIGRP Adjacency Changes (Level 2, Scorable)

Description:
Enable logging of EIGRP routing neighbor changes.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to disable all interfaces from sending and receiving routing updates by default...

```
hostname(config)# router eigrp <virtual-instance-name>
```

```
hostname(config)# eigrp log-neighbor-changes
```

Audit:
Perform the following to determine if this is set properly:

```
hostname# sh run | beg router eigrp
```

Default Value:
EIGRP adjacency changes are not logged by default.

References:

1. Cisco Enterprise Branch
2. Cisco IOS IP Routing: EIGRP Configuration Guide, Release 15.0

1.1.2.2 Log OSPF Adjacency Changes (Level 2, Scorable)

Description:
Enable logging of OSPF routing neighbor changes.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to disable all interfaces from sending and receiving routing updates by default...

```
hostname(config)# router ospf <ospf_process-id>
hostname(config)# ospf log-neighbor-changes
```

Audit:
Perform the following to determine if this is set properly:

```
hostname# sh run | beg router ospf
```

Default Value:
OSPF adjacency changes are not logged by default.

References:

1. Cisco Enterprise Branch
2. Cisco IOS IP Routing: OSPF Configuration Guide, Release 15.0

1.1.2.3 Log BGP Adjacency Changes (Level 2, Scorable)

Description:
Enable logging of BGP routing neighbor changes.

Platform:
IOS

Dependencies:

IOS: None

Remediation:
Perform the following to disable all interfaces from sending and receiving routing updates by default...

```
hostname(config)# router bgp <BGP_AS_number>
hostname(config)# bgp log-neighbor-changes
```

Audit:
Perform the following to determine if this is set properly:

```
hostname# sh run | beg router bgp
```

Default Value:
BGP adjacency changes are not logged by default.

References:
1. Cisco Enterprise Branch
2. Cisco IOS IP Routing: BGP Configuration Guide, Release 15.0

1.2 Switch Protections

Description:
This section focuses on items that provide additional local switch protections.

1.2.1 Enable Spanning Tree (Level 1, Scorable)

Description:
Spanning tree protocol (STP) is a layer 2, loop detection and control protocol. Each organization needs to evaluate the advantages and disadvantages prior to architecting and deploying spanning tree.

Cisco has several STP options – Per-VLAN Spanning Tree+ (PVST+), Multiple Spanning Tree (MST), and Rapid Per-VLAN Spanning Tree+ (Rapid-PVST+).

PVST+ is a Cisco proprietary version of STP that creates an STP instance per VLAN. Other networking equipment companies do support this version of the protocol – most of which have limitations.

MST is an IEEE standard (previously 802.11s but now merged into 802.1q-2005) that combines all BPDU (Bridge Protocol Data Units) into a single format.

Rapid-PVST+ is a Cisco proprietary version of STP that combines the functionality of PVST and RSTP (Rapid Spanning Tree Protocol).

Rationale:
By enabling spanning tree, the administrator can provide protection from (un-)intentional broadcast storms arising from a switching loop.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to enable spanning tree…

```
hostname(config)# spanning-tree mode {pvst | mst | rapid-pvst}
```

Audit:
Perform the following to determine spanning tree is set properly:

```
hostname# sh run | incl spanning-tree
```

Default Value:
PVST+ is enabled by default when implementing spanning tree.

References:
1. Cisco IOS LAN Switching Command Reference, Release 15.0

1.2.2 Enable DHCP Snooping (Level 2, Scorable)

Description:
DHCP snooping provides options in restricting the impact of various types of DHCP attacks.

Rationale:
By enabling DHCP snooping, the network administrator can provide protection from items such as rogue or unintentionally installs DHCP servers, spoofing of DHCP server responses, and starvation attacks.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to enable DHCP snooping globally…

```
hostname(config)# ip dhcp snooping
```

Audit:
Perform the following to determine spanning tree is set properly:

```
hostname# sh ip dhcp snooping
```

Default Value:
DHCP protection is disabled by default.

References:

1. Configuring DHCP Features and IP Source Guard

1.2.2.1 Define a Trusted DHCP Interface (Level 2, Scorable)

Description:
Determine and define a trusted interface that DHCP server responses should come from.

Rationale:
This is one of several methods possible to do DHCP snooping. While this may not be the most secure method, it is an easier way to manage distribution level switches.

Platform:
IOS

Dependencies:
IOS: **1.3.2 Enable DHCP Snooping**

Remediation:
Perform the following to enable a trusted interface for DHCP responses…

```
hostname(config)# int <interface>
hostname(config-if)# ip dhcp snooping trust
```

Audit:
Perform the following to determine if DHCP snooping on a trusted interface is set properly:

```
hostname# sh ip dhcp snooping
```

Default Value:
DHCP protection is disabled by default.

References:

1. Configuring DHCP Features and IP Source Guard

1.2.2.2 Limit the Number of DHCP Packet per Second (Level 2, Scorable)

Description:
Limit the number of DHCP packets per section that an interface will accept.

Rationale:
Cisco recommends limiting DHCP packets to no more than 100 packets per second.

Platform:
IOS

Dependencies:
IOS: **1.3.2 Enable DHCP Snooping**

Remediation:
Perform the following to enable a trusted interface for DHCP responses…

```
hostname(config)# int <interface>
hostname(config-if)# ip dhcp snooping limit rate <rate>
```

Audit:
Perform the following to determine if the DHCP snooping rate limit is set properly:

```
hostname# sh ip dhcp snooping
```

Default Value:
DHCP snooping rate limiting is disabled by default.

References:

1. Configuring DHCP Features and IP Source Guard

1.2.3 Enable Dynamic ARP Inspection (Level 2, Scorable)

Description:
Dynamic ARP inspection provides a method to defeat ARP poisoning attacks.

Rationale:
ARP spoofing is typically trivial to execute. Dynamic ARP inspection intercepts all ARP requests from untrusted interfaces, validates the IP-to-MAC mapping, and drops invalid ARP packets.

Platform:
IOS

Dependencies:
IOS: **1.3.2 Enable DHCP Snooping**

Remediation:
Perform the following to enable per-VLAN ARP inspection…

```
hostname(config)# ip arp inspection vlan <vlan-range>
```

Audit:
Perform the following to determine ARP inspection is set properly:

```
hostname# show ip arp inspection vlan <vlan-range>
```

Default Value:
Dynamic ARP inspection is disabled by default.

References:

1. Configuring DHCP Features and IP Source Guard

1.2.3.1 Enable Dynamic ARP Inspection Trusted Interface (Level 2, Scorable)

Description:
Define a trusted interface – typically the uplink.

Rationale:
By defaults, all interfaces are untrusted. Defining a trusted interface allows the switch to pass the ARP packet without inspection.

Platform:

IOS

Dependencies:
IOS: **1.3.2 Enable DHCP Snooping**

Remediation:
Perform the following to enable a trusted interface…

```
hostname(config)# int <interface>
hostname(config-if)# ip arp inspection trust
```

Audit:
Perform the following to determine if the trusted interface is set properly:

```
hostname# show ip arp inspection interfaces
```

Default Value:
Dynamic ARP inspection is disabled by default.

References:
1. Configuring DHCP Features and IP Source Guard

1.3 VPN Backup Link (Levels 1 and 2, Scorable)

Description:
Setup a backup using a Virtual Private Network (VPN).

Rationale:
Using a VPN as a backup link provides link redundancy by having a second path back to the main network – typically one (or more) IPSEC tunnels traversing the Internet.

Platform:
IOS

Dependencies:
IOS: None

1.3.1 Static Site-to-Site VPN (Levels 1 and 2, Scorable)

1.3.1.1 Create a IKEv1 Policy (Level 1, Scorable)

Description:
Create a policy which defines the parameters for the IKE negotiation.

Rationale:
Ensure the use of sufficient encryption and hashing algorithms, RSA group, and authentication method to protect the IKE SA negotiation.

NOTE: This example only covers pre-shared key authentication. Cisco also offers several asynchronous measures as well.

Platform:

IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the ISAKMP policy…

```
hostname(config)# crypto isakmp policy <isakmp_policy_number>
```

Audit:
Perform the following to determine ARP inspection is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
There is no ISAKMP policy by default.

References:
1. Cisco IOS Security Command Reference

1.3.1.1.1 Set ISAKMP Encryption Level (Level 1, Scorable)

Description:
Set the encryption level for IKE negotiation.

Rationale:
Ensure the encryption algorithm is sufficient to protect the IKE negotiation to the level necessary for the organization.
Minimum: AES128

Recommended: AES256

Platform:
IOS

Dependencies:
IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the encryption level…

```
hostname(config-isakmp)# encryption <des | 3des | aes | aes192 |
aes256>
```

Audit:
Perform the following to determine if the encryption is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
There is no ISAKMP policy by default.

References:
1. Cisco IOS Security Command Reference

2. NSA Suite B Cryptography

1.3.1.1.2 Set ISAKMP Hash (Level 1, Scorable)

Description:
Set the hash algorithm for ISAKMP.

Rationale:
Ensure the hash algorithm is sufficient to protect the IKE negotiation to the level necessary for the organization.

Minimum: SHA256

Recommended: SHA384

Platform:
IOS

Dependencies:
IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the encryption level…

```
hostname(config-isakmp)# hash <sha | sha256 | sha384 | md5>
```

Audit:
Perform the following to determine if the hash algorithm is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
SHA1 is the default when not explicitly configured in an ISAKMP policy.

References:
1. Cisco IOS Security Command Reference
2. NSA Suite B Cryptography

1.3.1.1.3 Set Authentication Type (Level 1, Scorable)

Description:
Set the authentication type for the ISAKMP exchange.

Rationale:
Cisco provides the ability to authenticate the ISAKMP exchange using a pre-shared key or through the use of public key infrastructure (PKI).

As not all organizations have a trusted, internal PKI infrastructure, the subsequent configurations in this guide uses pre-shared keys.

Platform:
IOS

Dependencies:
IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the encryption level…

```
hostname(config-isakmp)# auth <rsa-sig | rsa-encr | pre-share | ecdsa-
sig>
```

Audit:
Perform the following to determine if the hash algorithm is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
RSA signature authentication is the default when not explicitly configured in an ISAKMP policy.

References:
1. Cisco IOS Security Command Reference

1.3.1.1.4 Set the Diffie-Hellman Group (Level 1, Scorable)

Description:
Set the Diffie-Hellman (DF) Group for the IKEv1 exchange.

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group

Rationale:
The DF should be sufficiently strong to protect the IPSec keys during the exchange.

Minimum: Group 14 – 2048-bit DH group

Recommended: Group 19 – 256-bit elliptic curve DH (ECDH) group

Platform:
IOS

Dependencies:

IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the encryption level…

```
hostname(config-isakmp)# group <df_group_number>
```

Audit:
Perform the following to determine if the hash algorithm is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
Group 1 is the default when not explicitly configured in the ISAKMP policy.

References:
1. Cisco IOS Security Command Reference
2. NSA Suite B Cryptography

1.3.1.1.5 Set Perfect Forward Secrecy for the Diffie-Hellman Group (Level 2, Scorable)

Description:
Perfect forward secrecy requires a new Diffie-Hellman (DH) key exchange each time the tunnel computes encryption and/or authentication keys.

Set Perfect Forward Secrecy for the DH Group for the IKEv1 exchange.

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group

Rationale:
By requiring a new DH exchange, this will limit data compromise to only that of the lifetime of the previous DH exchange. The DH group should be sufficiently strong to protect the IPSec keys during the exchange.

Minimum: PFS with Group 14 – 2048-bit DH group

Recommended: PFS with Group 19 – 256-bit elliptic curve DH (ECDH) group

Platform:
IOS

Dependencies:
IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the encryption level…

```
hostname(config-isakmp)# set pfs <df_group_number>
```

Audit:
Perform the following to determine if the hash algorithm is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
Group 1 is the default when not explicitly configured in the ISAKMP policy.

References:
1. Cisco IOS Security Command Reference
2. NSA Suite B Cryptography

1.3.1.1.6 Set the Lifetime of the IKEv1 SA (Level 1, Scorable)

Description:
Set the lifetime for the ISAKMP SA.

Rationale:
The lifetime determines when the IKE Security Association (SA) expires. Ensure to balance having a shorter expiration time to limit the exposure to attacks directed at the SA with a longer lifetime to limit the number IKE SA negotiation times.

Minimum: 84600 second (default)

Recommended: 28800 seconds

Platform:
IOS

Dependencies:
IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the IKEv1 SA timeout…

```
hostname(config-isakmp)# lifetime <seconds>
```

Audit:
Perform the following to determine if the hash algorithm is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:

86,400 seconds is the default when not explicitly configured in the ISAKMP policy.

References:
1. Cisco IOS Security Command Reference

1.3.1.2 Create an IKEv2 Proposal (Level 2, Scorable)

Description:
Create a proposal which defines the parameters for the IKEv2 negotiation.

Rationale:
Ensure the use of sufficient encryption and hashing algorithms, RSA group, and authentication method to protect the IKEv2 SA negotiation.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the IKEv2 proposal…

```
hostname(config)# crypto ikev2 proposal <ikev2_proposal_name>
```

Audit:
Perform the following to determine if the proposal is set properly:

```
hostname# show crypto ikev2 proposal
```

Default Value:
There is no IKEv2 proposal by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.2.1 Set IKEv2 Proposal Encryption Algorithm(s) (Level 2, Scorable)

Description:
Create an IKEv2 proposal encryption

Rationale:
Ensure the encryption algorithm is sufficient to protect the IKE negotiation to the level necessary for the organization.

Minimum: AES128

Recommended: AES256

Platform:
IOS

Dependencies:
IOS: **1.4.2 Create an IKEv2 Proposal**

Remediation:
Perform the following to configure the ISAKMP policy…

```
hostname(config-ikev2-proposal)# encryption { 3des | aes-cbc-128 | aes-
cbc-192 | aes-cbc-256 }
```

Audit:
Perform the following to determine ARP inspection is set properly:

```
hostname# show crypto ikev2 proposal
```

Default Value:
AES-CBC-128 and along with 3DES is the default when not explicitly configured in an IKEv2 Proposal.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)
3. NSA Suite B Cryptography

1.3.1.2.2 Set IKEv2 Proposal Integrity Algorithm(s) (Level 2, Scorable)

Description:
Create an IKEv2 integrity algorithm.

Rationale:
Ensure the hash algorithm is sufficient to protect the IKE negotiation to the level necessary for the organization.

Minimum: SHA256

Recommended: SHA384

Platform:
IOS

Dependencies:
IOS: **1.4.2 Create an IKEv2 Proposal**

Remediation:
Perform the following to configure the IKEv2 integrity algorithm…

```
hostname(config-ikev2-proposal)# integrity { sha1 | sha256 | sha384 |
sha512 | md5 }
```

Audit:
Perform the following to determine if the integrity algorithm is set properly:

```
hostname# show crypto ikev2 proposal
```

Default Value:

SHA1 along with MD5 is the default when not explicitly configured in an IKEv2 Proposal.

References:

1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)
3. NSA Suite B Cryptography

1.3.1.2.3 Set IKEv2 Proposal Diffie-Hellman Group(s) (Level 2, Scorable)

Description:
Set the Diffie-Hellman (DF) Group for the IKEv2 exchange.

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group

Rationale:
The DF should be sufficiently strong to protect the IPSec keys during the exchange.

Minimum: Group 14 – 2048-bit DH group

Recommended: Group 19 – 256-bit elliptic curve DH (ECDH) group

Platform:
IOS

Dependencies:
IOS: **1.4.2 Create an IKEv2 Proposal**

Remediation:
Perform the following to configure the IKEv2 integrity algorithm…

```
hostname(config-ikev2-proposal)# group { 1 | 2 | 5 | 14 | 15 | 16 | 19
| 20 | 24 }
```

Audit:
Perform the following to determine if the DF group is set properly:

```
hostname# show crypto ikev2 proposal
```

Default Value:

Group 2 along with Group 5 is the default when not explicitly configured in an IKEv2 Proposal.

References:

1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)
3. NSA Suite B Cryptography

1.3.1.2.4 Set Perfect Forward Secrecy for the Diffie-Hellman Group (Level 2, Scorable)

Description:
Perfect forward secrecy requires a new Diffie-Hellman (DH) key exchange each time the tunnel computes encryption and/or authentication keys.

Set Perfect Forward Secrecy for the DH Group for the IKEv1 exchange.

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group

Rationale:
By requiring a new DH exchange, this will limit data compromise to only that of the lifetime of the previous DH exchange. The DH group should be sufficiently strong to protect the IPSec keys during the exchange.

Minimum: PFS with Group 14 – 2048-bit DH group

Recommended: PFS with Group 19 – 256-bit elliptic curve DH (ECDH) group

Platform:
IOS

Dependencies:
IOS: **1.3.4.1 Create the ISAKMP Policy**

Remediation:
Perform the following to configure the encryption level…

```
hostname(config-isakmp)# set pfs <df_group_number>
```

Audit:
Perform the following to determine if the hash algorithm is set properly:

```
hostname# show crypto isakmp policy
```

Default Value:
Group 1 is the default when not explicitly configured in the ISAKMP policy.

References:

1. Cisco IOS Security Command Reference
2. NSA Suite B Cryptography

1.3.1.3 Create a IKEv2 Policy (Level 2, Scorable)

Description:
Create an IKEv2 policy

Rationale:
The IKEv2 policy

Platform:
IOS

Dependencies:
IOS: **1.4.2 Create an IKEv2 Proposal**

Remediation:
Perform the following to configure the IKEv2 proposal…

```
hostname(config)# crypto ikev2 policy <ikev2_policy_name>
```

Audit:
Perform the following to determine ARP inspection is set properly:

```
hostname# show crypto ikev2 policy
```

Default Value:
There is no IKEv2 proposal by default.

References:

1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.3.1.1 Set the IKEv2 Policy Proposal (Level 2, Scorable)

Description:
Set the proposal for the IKEv2 policy.

Rationale:
This is a required step to the IKEv2 setup process.

Platform:

IOS

Dependencies:
IOS: **1.4.2.4 Create a IKEv2 Policy**

Remediation:
Perform the following to configure the IKEv2 proposal…

```
hostname(config-ikev2-policy)# proposal <ikev2_proposal_name>
```

Audit:
Perform the following to determine if the IKEv2 policy proposal is set properly:

```
hostname# show crypto ikev2 policy
```

Default Value:
There is no IKEv2 policy proposal by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.3.1.2 Set the IKEv2 Policy Match Criteria (Level 2, Scorable)

Description:
Set the match criteria for the IKEv2 policy.

Rationale:
The match criteria determines which local address(es) to use.

Platform:
IOS

Dependencies:
IOS: **1.4.2.4 Create a IKEv2 Policy**

Remediation:
Perform the following to configure the IKEv2 proposal…

```
hostname(config-ikev2-policy)# match local {ipv4-address | ipv6-address
| fvrf fvrf-name | any}
```

Audit:
Perform the following to determine if the match criteria are set properly:

```
hostname# show crypto ikev2 policy
```

Default Value:
All local addresses are permitted by default when not explicitly configured in an IKEv2 Proposal.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.4 Create an IKEv2 Keyring (Level 2, Scorable)

Description:
Create an IKEv2 keyring.

Rationale:
The IKEv2 keyring allows the use of local or remote authenticated pre-shared keys.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the IKEv2 proposal…

```
hostname(config)# crypto ikev2 keyring <ikev2_keyring_name>
```

Audit:
Perform the following to determine if the IKEv2 keyring is set properly:

```
hostname# show crypto ikev2 policy
```

Default Value:
There is no IKEv2 keyring by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.4.1 Set the IKEv2 Keyring Peer (Level 2, Scorable)

Description:
Set the IKEv2 keyring peer

Rationale:
The IKEv2 keyring allows definition of one or more peers.

Platform:
IOS

Dependencies:
IOS: **1.4.2.5 Create an IKEv2 Keyring**

Remediation:
Perform the following to configure the IKEv2 proposal…

```
hostname(config-ikev2-keyring)# peer <peer_name>
```

Audit:
Perform the following to determine if the peer name is set properly:

```
hostname# show crypto ikev2 profile
```

Default Value:
There is no IKEv2 keyring peer by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.4.1.1 Set the Peer Description (Level 2, Scorable)

Description:
Set the IKEv2 keyring peer description.

Rationale:
It is useful to provide a description of the keyring peer to aid in setup and troubleshooting.

Platform:
IOS

Dependencies:
IOS: **1.4.2.5.1 Set the IKEv2 Keyring Peer**

Remediation:
Perform the following to configure the peer description…

```
hostname(config-ikev2-keyring-peer)# description <peer_description>
```

Audit:
Perform the following to determine if the peer description is set properly:

```
hostname# show crypto ikev2 profile
```

Default Value:
There is no peer description by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.4.1.2 Set the Peer Address (Level 2, Scorable)

Description:
Set the IKEv2 keyring peer address.

Rationale:
This limits the IKEv2 negotiation to between specific peers.

Platform:
IOS

Dependencies:
IOS: **1.4.2.5.1 Set the IKEv2 Keyring Peer**

Remediation:

Perform the following to configure the peer description…

```
hostname(config-ikev2-keyring-peer)# address <peer_ip_address>
```

Audit:
Perform the following to determine if the peer description is set properly:

```
hostname# show crypto ikev2 profile
```

Default Value:
There is no peer address by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.4.1.3 Set the Pre-Shared Key (Level 2, Scorable)

Description:
Set the IKEv2 keyring pre-shared key.

Rationale:
It is necessary to create a key of sufficient complexity to deter guessing.

NOTE: This key will show in clear-text in the configuration.

Platform:
IOS

Dependencies:
IOS: **1.4.2.5.1Set the IKEv2 Keyring Peer**

Remediation:
Perform the following to configure the peer description…

```
hostname(config-ikev2-keyring-peer)# pre-shared-key <key>
```

Audit:
Perform the following to determine if the peer description is set properly:

```
hostname# show crypto ikev2 profile
```

Default Value:
There is no pre-shared key set by default.

References:
1. Cisco IOS Security Command Reference
2. Configuring Internet Key Exchange Version 2 (IKEv2)

1.3.1.5 Define the ISAKMP Key (Level 1, Scorable)

Description:
Define the ISAKMP pre-shared key which the peer's will use to authenticate each other.

Rationale:
Since this key controls authentication between peers, it is necessary to create a key of sufficient complexity to deter guessing.

NOTE: This key will show in clear-text in the configuration.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the ISAKMP key…

```
hostname(config)# crypto isakmp key <key_string> <peer_ip_address>
```

Audit:
Perform the following to determine if the proposal is set properly:

```
hostname# show crypto isakmp key
```

Default Value:
There is no ISAKMP key set by default.

References:
1. Cisco IOS Security Command Reference

1.3.1.6 Define the IPSEC Transform Set (Level 1, Scorable)

Description:
Define the IPSEC transform set.

Rationale:
The transform set specifies the IPSEC security protocol(s) and other algorithms and settings to apply to traffic protected by IPSEC.

ESP providing confidentiality protection in addition to AES128 (minimum) or AES256 (recommended).

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the transform set…

```
hostname(config)# crypto ipsec transform-set <transform_set_name>
{transform_option}
```

Audit:

Perform the following to determine if the proposal is set properly:

```
hostname# show crypto ipsec transform-set
```

Default Value:
There is no transform set by default.

References:
1. Cisco IOS Security Command Reference
2. NSA Suite B Cryptography

1.3.1.7 Define the Match ACL (Level 1, Scorable)

Description:
Define the ACL that the crypto map will use to determine which traffic to protect.

Rationale:
This is a required step to the crypto map process.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config)# ip access-list extended <match_acl_name>
hostname(config-nacl)# permit ip <source_network> <source_network_mask>
<destination_network> <destination network_mask>
```

Audit:
Perform the following to determine if the peer is set properly:

```
hostname# show ip access-list <match_acl_name>
```

Default Value:
There is no peer set by default.

References:
1. Cisco IOS Security Command Reference

1.3.1.8 Define the IPSEC Security Association Lifetime (Level 1, Scorable)

Description:
Define the IPSEC security association (SA) lifetime.

Rationale:
The lifetime determines when the IPSEC Security Association (SA) expires. Ensure to balance having a shorter expiration time to limit the exposure to attacks directed at the SA with a longer lifetime to limit the number of times the equipment goes through an IPSEC SA negotiation.

Minimum: 3600 second (default)

Recommended: Time in seconds acceptable to match organization security policy

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the global crypto map…

```
hostname(config)# crypto ipsec security-association lifetime
<lifetime_in_seconds>
```

Audit:
Perform the following to determine if the proposal is set properly:

```
hostname# show crypto ipsec security-association lifetime
```

Default Value:
There is no transform set by default.

References:
1. Cisco IOS Security Command Reference

1.3.1.9 Define the Global Crypto Map (Level 1, Scorable)

Description:
Define the global crypto map.

Rationale:
The crypto map defines items such as which traffic to protect, IPSEC peers, transform sets, and key and SA management.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the global crypto map…

```
hostname(config)# crypto map <crypto_map_name> <sequence_number> ipsec-
isakmp
```

Audit:
Perform the following to determine if the proposal is set properly:

```
hostname# show crypto map
```

Default Value:

There is no transform set by default.

References:

1. Cisco IOS Security Command Reference

1.3.1.9.1 Define the IPSEC Peer IP (Level 1, Scorable)

Description:
Define the global crypto map.

Rationale:
The transform

Platform:
IOS

Dependencies:
IOS: **1.3.6 Define the Global Crypto Map**

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config-crypto-map)# set peer <peer_ip_address>
```

Audit:
Perform the following to determine if the peer is set properly:

```
hostname# show crypto map
```

Default Value:
There is no peer set by default.

References:

1. Cisco IOS Security Command Reference

1.3.1.9.2 Define the IPSEC Transform Set (Level 1, Scorable)

Description:
Define the transform set.

Rationale:
The transform set

Platform:
IOS

Dependencies:
IOS: **1.3.6 Define the Global Crypto Map**

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config-crypto-map)# set transform-set <transform_set_name>
```

Audit:
Perform the following to determine if the peer is set properly:

```
hostname# show crypto map
```

Default Value:
There is no transform set by default.

References:
1. Cisco IOS Security Command Reference

1.3.1.9.3 Apply the IPSEC Match ACL (Level 1, Scorable)

Description:
Apply the ACL that the crypto map will use to determine which traffic to protect.

Rationale:
The transform

Platform:
IOS

Dependencies:
IOS: **1.3.5 Define the Match ACL**

1.3.6 Define the Global Crypto Map

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config-crypto-map)# match address <match_acl_name>
```

Audit:
Perform the following to determine if the peer is set properly:

```
hostname# show crypto map
```

Default Value:
There is no match address set by default.

References:
1. Cisco IOS Security Command Reference

1.3.1.10 Apply the Crypto Map to the Interface (Level 1, Scorable)

Description:
Configure the appropriate interface to activate IPSec protection.

Rationale:
The transform

Platform:
IOS

Dependencies:

IOS: **1.4.4 Define the Global Crypto Map**

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config-if)# crypto map <crypto_map_name>
```

Audit:
Perform the following to determine if the peer is set properly:

```
hostname# sh int
```

Default Value:
There is no interface crypto map set by default.

References:
1. Cisco IOS Security Command Reference

1.3.2 DMVPN Spoke Backup Link (Level 2, Scorable)

Description:
Setup a backup using a Virtual Private Network (VPN) using Dynamic Multipoint VPN (DMVPN).

Rationale:
DMVPN uses generic routing encapsulation (GRE), IPSEC, and Next Hop Resolution Protocol (NHRP). DMVPN provide better scaling for large and small IPSEC VPNs.

Platform:
IOS

Dependencies:
IOS: **1.3.1.1 Create a IKEv1 Policy (Full section completed)**

1.3.2 Define the ISAKMP Key

1.3.2.1 Create the IPSEC Profile (Level 2, Scorable)

Description:
Create the IPSEC profile that DMVPN will use to apply IPSEC protection to the GRE tunnel.

Rationale:
This is a required step to setup DMVPN.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config)# crypto ipsec profile <ipsec_profile_name>
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh run | incl ipsec profile
```

Default Value:
There is no IPSEC profile configured by default.

References:
1. Cisco IOS Security Command Reference

1.3.2.1.1 Set the Transform Set (Level 2, Scorable)

Description:
Set the IPSEC transform set that the IPSEC profile will use.

Rationale:
This is a required step to setup DMVPN.

Platform:
IOS

Dependencies:
IOS: **1.3.3 Define the IPSEC Transform Set**

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config)# set transform-set <ipsec_profile_name>
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh crypto ipsec transform-set
```

Default Value:
There is no IPSEC profile transform-set configured by default.

References:
1. Cisco IOS Security Command Reference

1.3.2.2 Create a Tunnel Interface (Level 2, Scorable)

Description:
This tunnel interface will become the GRE tunnel.

Rationale:
This is a required step to setup DMVPN.

Platform:
IOS

Dependencies:
IOS: None

Remediation:
Perform the following to configure the global crypto peer IP…

```
hostname(config)# interface tunnel<tunnel_number>
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh int
```

Default Value:
There are no tunnel interfaces by default.

References:
1. Cisco IOS Interface and Hardware Component Command Reference

1.3.2.2.1 Create a Tunnel IP address (Level 2, Scorable)

Description:
Assign an IP address to the tunnel interface.

Rationale:
This is the GRE tunnel IP address that DMVPN will use to establish a connection to the hub and/or other spoke locations.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the tunnel IP address…

```
hostname(config-if)# ip address <tunnel_ip_address> <tunnel_mask>
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no tunnel IP address by default.

References:
1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.2 Reduce the Tunnel MTU (Level 2, Scorable)

Description:
The maximum transmission unit (MTU) determines the size of the IP packet.

Rationale:

Due to tunnel overhead, you will need to reduce the MTU to reduce performance and compatibility issues.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the tunnel MTU…

```
hostname(config-if)# ip mtu <mtu_size>
```

Audit:
Perform the following to determine if the tunnel MTU is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
The default MTU is 1500 bytes for an Ethernet interface.

References:
1. Cisco IOS IP Application Services Command Reference

1.3.2.2.3 Set NHRP Authentication String (Level 2, Scorable)

Description:
The authentication string must be the same amongst all NHRP.

Rationale:
NHRP authentication allows the peer's to authenticate each other and communicate.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the tunnel IP address…

```
hostname(config-if)# ip nhrp authentication <nhrp_auth_string>
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no NHRP authentication by default.

References:
1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.4 Set the NHRP to Allow Dynamic Tunnels (Level 2, Scorable)

Description:
Setup the router to allow dynamic spoke-to-spoke DMVPN connections.

Rationale:
This command is necessary to create dynamic tunnels.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure dymanic tunneling for NHRP …

```
hostname(config-if)# ip nhrp map multicast dynamic
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no dynamic tunneling for NHRP by default.

References:
1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.5 Set the NHRP Hub Map (Level 2, Scorable)

Description:
Setup the router to map the destination IP to the respective IP-to-nonbroadcast IP address.

Rationale:
This command is necessary to map to the Hub.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure dymanic tunneling for NHRP …

```
hostname(config-if)# ip nhrp map <destination_ip> <nmba_ip>
```

Audit:
Perform the following to determine if the tunnel is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:

There is no NHRP map set by default.

References:

1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.6 Set the NHRP to Allow Hub Multicast (Level 2, Scorable)

Description:
Setup the router to allow dynamic routing to Hub DMVPN connections.

Rationale:
Certain protocols require GRE to communicate across a WAN or the Internet.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure multicast support for NHRP …

```
hostname(config-if)# ip nhrp map multicast <nmba_ip>
```

Audit:
Perform the following to determine if multicast support is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no multicast for NHRP by default.

References:

1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.7 Set the NHRP Network ID (Level 2, Scorable)

Description:
Setup a logical NBMA network identifier.

Rationale:
All endpoints within the NBMA must have the same network identifier.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the NHRP network identifier…

```
hostname(config-if)# ip nhrp network-id <id_number>
```

Audit:
Perform the following to determine if the NHRP network identifier is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no NHRP network identifier set by default.

References:
1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.8 Set the NHS IP (Level 2, Scorable)

Description:
Specify the next hop router.

Rationale:
All endpoints within the NBMA must have the same network identifier.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the NHRP network identifier…

```
hostname(config-if)# ip nhrp nhs <nhs_ip_address>
```

Audit:
Perform the following to determine if the NHRP network identifier is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no NHS IP set by default.

References:
1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.9 Set the Tunnel Source (Level 2, Scorable)

Description:
Specify the tunnel source interface.

Rationale:
The NHRP tunnel requires a source interface.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the NHRP network identifier…

```
hostname(config-if)# tunnel source <source_interface>
```

Audit:
Perform the following to determine if the NHRP network identifier is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no source interface set by default.

References:
1. Cisco IOS IP Addressing Services Command Reference

1.3.2.2.10 Set the Tunnel Key (Level 2, Scorable)

Description:
Specify the tunnel key.

Rationale:
The tunnel key provides an additional, but weak, security requirement to reduce the likelihood of issues due to an improperly configured tunnel or packet injection.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

Remediation:
Perform the following to configure the tunnel mode…

```
hostname(config-if)# tunnel key <key_number>
```

Audit:
Perform the following to determine if the tunnel mode is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no tunnel key set by default.

References:
1. Cisco IOS Interface and Hardware Component Command Reference

1.3.2.2.11 Set the Tunnel Protection (Level 2, Scorable)

Description:
Specify the tunnel protection.

Rationale:
Tunnel protection specifies the type of IPSEC encryption that will applied to the tunnel.

Platform:
IOS

Dependencies:
IOS: **1.3.8.1 Create a Tunnel Interface**

1.3.2.1Create the IPSEC Profile

Remediation:
Perform the following to configure the tunnel mode…

```
hostname(config-if)# tunnel protection ipsec profile
<ipsec_profile_name>
```

Audit:
Perform the following to determine if the tunnel mode is set properly:

```
hostname# sh run int tu<tunnel_number>
```

Default Value:
There is no tunnel protection set by default.

References:
1. Cisco IOS Security Command Reference

Appendix A: References

1. Cisco Systems, Inc. (2010). Cisco Enterprise Branch. http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap8.html. Last accessed August 18, 2011
2. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: EIGRP Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-cr-book.html. Last accessed August 18, 2011.
3. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: OSPF Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/iproute_ospf/command/reference/iro_book.html. Last accessed August 18, 2011.
4. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: BGP Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html. Last accessed June 28, 2011.
5. Cisco Systems, Inc. (2010). Cisco IOS LAN Switching Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_book.html. Last accessed August 18, 2011.
6. Cisco Systems, Inc. (2008). Configuring DHCP Features and IP Source Guard. http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_46_se/configuration/guide/swdhcp82.html. Last accessed August 23, 2011.
7. Cisco Systems, Inc. (2008). Configuring Dynamic ARP Inspection. http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_46_se/configuration/guide/swdynarp.html. Last accessed August 23, 2011.
8. Cisco Systems, Inc. (2011). Cisco IOS Security Command Reference. http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. Last accessed September 4, 2011.
9. Cisco Systems, Inc. (2011). Configuring Internet Key Exchange Version 2 (IKEv2). http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html. Last accessed September 6, 2011.
10. National Security Agency (2010). NSA Suite B Cryptography. http://www.nsa.gov/ia/programs/suiteb_cryptography. Last accessed October 6, 2011.
11. Cisco Systems, Inc. (2008). Dynamic Multipoint VPN (DMVPN) Design Guide. http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPNttl.html. Last accessed October 6, 2011.
12. Cisco Systems, Inc. (2010). Cisco IOS Interface and Hardware Component Command Reference. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-cr-book.html. Last accessed October 13, 2011.
13. Cisco Systems, Inc. (2010). Cisco IOS IP Addressing Services Command Reference. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html. Last accessed October 13. 2011.

14. Cisco Systems, Inc. (2010). Cisco IOS IP Application Services Command Reference. http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/command/iap-cr-book.html. Last accessed October 13, 2011.

Appendix B: Change History

Date	Version	Changes for this version
August 18, 2011	0.1	Initial draft development – routing and switching
August 23, 2011	0.2	Added DHCP and ARP snooping sections
September 4, 2011	0.3	Started VPN sections
September 6, 2011	0.4	Completed IKEv1 and v2 sections
September 29, 2011	0.5	Completed crypto map sections and reviewed (and updated) all sections
October 6, 2011	0.5.1	Updated Encryption, Hashing, and DH minimums and recommendeds
October 6, 2011	0.5.1	Added PFS
October 13, 2011	0.6	Added DMVPN Spoke sections
October 18, 2011	1.0.0-A1	Added missing DMVPN section, added IPSEC SA lifetime