the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Cisco Firewall VPN Services

Version 1.0.0

December 31, 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 Firewall VPN Services 1.0* provides prescriptive guidance for establishing a secure configuration posture for *Cisco Firewalls* versions *7.2 – 8.4* running on *Cisco ASA.* This guide was tested against *Cisco ASA 8.4* installed by asa842-k8.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 *Security Configuration Benchmark for Firewall VPN Services 1.0.0* on a Cisco ASA platform.

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:

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

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

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
Ashwin Kohli
Slava Kurenyshev
Andy McConnell, *Tripwire, Inc.*
Tim Muniz, *Tenable Network Security, Inc.*
Jason Nehrboss, *Computer Sciences Corporation*
Justin Opatrny
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 Remote Access IPSEC VPN (Levels 1 and 2, Scorable)

Description:
IPSEC is a common technology that is used to provide secure communication for remote workers over the public Internet.

Rationale:
Configuration of a remote access VPN should be accomplished in a manner that will provide maximum confidentiality and integrity for sensitive information.

Platform:
FW

Dependencies:
FW: None

1.1.1 Create an 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:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure the ISAKMP policy:

```
hostname(config)# crypto ikev1 policy priority
```

Audit:
Perform the following to determine IKEv1 policy configuration:

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

Default Value:
There is no ISAKMP policy by default.

Additional References:

1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.1 Set IKEv1 Authentication type (Level 1, Not Scorable)

Description:
Set the authentication type for the ISAKMP exchange.

Rationale:
The device can be configured 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:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev1-policy))# authentication {crack | pre-share |
rsa-sig}
```

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. Pre-share authentication is the default when not explicitly configured in the ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.2 Set IKEv1 Encryption Level (Level 1, Scorable)

Description:
Set the encryption level for IKE negotiation to AES or greater.

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

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev1-policy)# encryption
{aes | aes-192 | aes-256}
```

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. 3des encryption is the default when not explicitly configured in an ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.3 Set IKEv1 Hash (Level 1, Scorable)

Description:
Set the ISAKMP hash algorithm to SHA-1 or greater.

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

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev1-policy)# hash sha
```

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

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

Default Value:
There is no ISAKMP policy by default. SHA-1 is the default has algorithm when not explicitly configured in an ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.4 Set IKEv1 Diffie-Hellman Group (Level 1, Scorable)

Description:
Set the Diffie-Hellman (DF) Group for the IKEv1 exchange to Group 2 or greater.

1 Specifies the 768-bit DH group

2 Specifies the 1024-bit DH group

5 Specifies the 1536-bit DH group

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

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev1-policy)# group
{2 | 5}
```

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

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

Default Value:
There is no ISAKMP policy by default. Group 2 is the default when not explicitly configured in the ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.5 Set the IKEv1 SA Lifetime (Level 1, Scorable)

Description:
Set the lifetime for the ISAKMP Security Association (SA) to 3600 seconds or less.

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.

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

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

```
hostname(config-ikev1-policy)# lifetime
{3600}
```

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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.6 Configure IKEv1 Transform Set (Level 1, Scorable)

Description:
Define the IKEv1 transform set using Encapsulating Security Payload (ESP) - AES or greater.

Rationale:
The transform set specifies the IKEv1 encryption and hash mechanism to use in order to protect the IPSEC session establishment.

Platform:

FW

Dependencies:
FW: None

Remediation:
Perform the following to configure the transform set:

```
hostname(config)# crypto ipsec ikev1 transform-set transform-set-name
encryption-method [esp-aes | esp-aes-192 | esp-aes-256]
```

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

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

Default Value:
There is no IKEv1 transform set by default.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.1.7 Configure the IKEv1 Interface (Level 1, Scorable)

Description:
Set the firewall interface used to perform the ISAKMP exchange.

Rationale:
An external interface must be configured to terminate VPN connections and respond to ISAKMP key exchanges. More than one interface may be chosen to support the VPN process.

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config)# crypto ikev1 enable interface-name
```

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

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

Default Value:
None.

Additional References:
1. NSA Router Security Configuration Guide

2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2 Create an IKEv2 Policy (Level 1, Scorable)

Description:
Create a policy that 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 IKEv2 SA negotiation.

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

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure the ISAKMP policy:

```
hostname(config)# crypto ikev2 policy priority
```

Audit:
Perform the following to determine IKEv1 policy configuration:

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

Default Value:
There is no ISAKMP policy by default.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.1 Set IKEv2 Authentication type (Level 1, Not Scorable)

Description:
Set the authentication type for the IKEv2 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:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev2-policy))# authentication {crack | pre-share |
rsa-sig}
```

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. Pre-share authentication is the default when not explicitly configured in the ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.2 Set IKEv2 Encryption Level (Level 1, Scorable)

Description:
Set the encryption level for IKEv2 negotiation to AES or greater.

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

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev2-policy)# encryption {aes | aes-192 | aes-256}
```

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. 3des encryption is the default when not explicitly configured in the ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.3 Set IKEv2 Hash (Level 1, Scorable)

Description:
Set the hash algorithm for ISAKMP to SHA1 or greater.

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

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev2-policy)# hash {sha}
```

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

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

Default Value:
There is no ISAKMP policy by default. SHA-1 is the default hash algorithm when not explicitly configured in an ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.4 Set IKEv2 Diffie-Hellman Group (Level 1, Scorable)

Description:
Set the Diffie-Hellman (DF) Group for the IKEv1 exchange to Group 2 or greater.

1 Specifies the 768-bit DH group

2 Specifies the 1024-bit DH group

5 Specifies the 1536-bit DH group

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

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level:

```
hostname(config-ikev2-policy)# group {2 | 5}
```

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

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

Default Value:
Group 2 is the default when not explicitly configured in the ISAKMP policy.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.5 Set the IKEv2 SA Lifetime (Level 1, Scorable)

Description:
Set the lifetime for the ISAKMP SA to 3600 seconds or less.

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.

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

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

```
hostname(config-ikev2-policy)# lifetime {3600}
```

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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.6 Configure IKEv2 proposal (Level 1, Scorable)

Description:
Define the IKEv2 proposal.

Rationale:
The IKEv2 proposal specifies the encryption and integrity algorithms to use in order to protect the IPSEC session establishment.

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure the transform set:

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal proposal_name
```

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

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

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

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.7 Configure IKEv2 proposal encryption and integrity (Level 1, Scorable)

Description:

Define the IKEv2 proposal encryption and integrity algorithms using Encapsulating Security Payload (ESP) – AES and SHA-1 or greater.

Rationale:
The IKEv2 proposal specifies the IKEv2 encryption and hash mechanism to use in order to protect the IPSEC session establishment.

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure the transform set:

```
hostname(config-ipsec=proposal)# protocol {esp} {encryption {aes | aes-
192 | aes-256 | null} | integrity {sha-1}
```

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

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

Default Value:
There is no IKEv2 proposal defined by default. When defining an IKEv2 proposal, 3des is the default encryption and SHA-1 is the default integrity algorithm.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.2.8 Configure the IKEv2 Interface (Level 1, Not Scorable)

Description:
Set the firewall interface used to perform the IKEv2 exchange.

Rationale:
An external interface must be configured to terminate VPN connections and respond to IKEv2 key exchanges. More than one interface may be chosen to support the VPN process.

Platform:
FW

Dependencies:
FW: 1.1.1 Create an IKEv1 Policy

Remediation:
Perform the following to configure the encryption level...

```
hostname(config)# crypto ikev2 enable interface-name
```

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

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

Default Value:
None.

Additional References:

1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.3 Define the ISAKMP Key (Level 1, Scorable)

Description:
Define the ISAKMP pre-shared key that 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:
FW

Dependencies:
FW: 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.

Additional References:

1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.4 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 using AES or greater is recommended.

Platform:
FW

Dependencies:
FW: 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.5 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:
FW

Dependencies:
FW: 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.6 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:
FW

Dependencies:
FW: 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

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

Description:
Define the global crypto map.

Rationale:
The transform

Platform:
FW

Dependencies:
FW: 1.1.6 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

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

Description:
Define the transform set.

Rationale:
The transform set

Platform:
FW

Dependencies:
FW: 1.1.6 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.1.6.3 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:
FW

Dependencies:
FW: 1.1.5 Define the Match ACL
1.1.6 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

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

Description:
Configure the appropriate interface to activate IPSec protection.

Rationale:
The transform

Platform:
FW

Dependencies:

FW: 1.1.6 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.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.2 Remote Access SSL VPN (Levels 1 and 2, Scorable)

Description:
SSL is a commonly used VPN technology that provides secure communication for remote workers over the public Internet.

Rationale:
Configuration of a remote access SSL VPN should be accomplished in a manner that will provide maximum confidentiality and integrity for sensitive information.

Platform:
FW

Dependencies:
FW: None

1.2.1 Require a Valid Certificate (Level 1, Not Scorable)

Description:
A trusted and valid certificate is used to verify the Identity of an SSL termination point.

Rational:
The use of a trusted certificate can help reduce the likelihood of a man in the middle attack spoofing a fake certificate. It is common for self-signed certificates in lab environments, but should never be used for a production SSL VPN.

Platform:
FW

Dependencies:

FW: None

Remediation:
Configuration of a certificate is a multistep process that depends on the 3rd party certificate provider. Please refer to the device configuration documentation for more information.

Audit:
Perform the following to determine if a valid certificate is applied the external ASA interface:

```
hostname#show crypto ca certificates
```

Default Value:
A self-signed certificate is used by default.

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.2.2 Require the Latest Anyconnect Client Software (Level 1, Not Scorable)

Description:
The latest version of Anyconnect client software should be installed on the ASA and deployed to client machines.

Rational:
Ensures that bug and security fixes can be deployed to all clients when they connect to the SSL VPN through the automatic update mechanism.

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure the Anyconnect image after installing in flash memory:

```
hostname(config-webvpn)#anyconnect image <latest_image_pkg> 1
```

Audit:
Perform the following to determine if the current Anyconnect client software is configured:

```
hostname#show webvpn anyconnect
```

Default Value:
None. There are no Anyconnect images installed by default.

Additional References:

1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.2.3 Require SSL VPN Idle Timeout Value (Level 1, Scorable)

Description:
Configure an idle timeout for SSL VPN sessions. Set VPN idle timeout to 15 minutes or less.

Rational:
VPN idle timeout value will disconnect the SSL VPN session in the event that the user is idle for a period of time greater than defined by policy. Setting a short, session timeout reduces the risk of the authenticated session being hijacked by an unauthorized user.

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure SSL VPN idle timeout value:

```
hostname(config)#vpn-idle-timeout {minutes | none}
```

Audit:
Perform the following to verify VPN idle timeout value:

```
hostname#sh run group-policy | include vpn-idle-timeout
```

Default Value:
None

Additional References:

1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.2.4 Forbid Local Password Storage for SSL VPN Client (Level 1, Scorable)

Description:
Disable local password caching on the Anyconnect VPN client.

Rational:
Storing passwords locally allows anyone with access to the client to launch a VPN session without proving their identity.

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to disable local password caching:

```
hostname(config-group-policy)#password-storage disabled
```

Audit:
Perform the following to verify the VPN idle timeout:

```
hostname#sh run group-policy | include password-storage enable
```

Default Value:
Disabled

Additional References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.2.5 Require SSL Tunnel Rekey (Level 1, Scorable)

Description:
To improve security the SSL tunnel should be rekeyed and a new tunnel created. The rekey time should be 8 hours or less.

Rational:
Rekeying the SSL vpn tunnel will improve security through the initialization of a new tunnel, renegotiating cryptographic keys, and the initialization vector.

Platform:
FW

Dependencies:
FW: None

Remediation:
Perform the following to configure SSL VPN rekey method and timeout (timeout is expressed in minutes):

```
hostname(config-group-webvpn)#anyconnect SSL rekey method SSL
hostname(config-group-webvpn)#anyconnect SSL rekey time 240
```

Audit:
Perform the following to verify the SSL VPN rekey method and time:

```
hostname#sh run group-policy | include anyconnect ssl rekey
```

Default Value:

Disabled

Additional References:

1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.4
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

Appendix A: References

1. National Security Agency (2009). NSA Router Security Configuration Guide. http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf. Last accessed November 9, 2010.
2. United States Department of Justice (2009). US Department of Justice – Cybercrime – Appendix A - Sample Network Login Banner. http://www.cybercrime.gov/ssmanual/06ssma.html#AppA. Last accessed November 9, 2010.
3. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/config.html. Last accessed November 9, 2010.

Appendix B: Change History

Date	Version	Changes for this version
November 18, 2011	1.0.0-A1	Initial draft
December 2, 2011	1.0.0-A2	Added SSL VPN and final formatting
December 16, 2011	1.0.0-A3	Updated audit and remediation
Decemebr 31, 2011	1.0.0	Public Release