the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Cisco Firewall Internet Edge

Version 1.0.0

December 6, 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 Firewall*, provides prescriptive guidance for establishing a secure configuration posture for *Cisco Firewall* versions *8.2 – 8.4* running on *ASA and ASA SM* This guide was tested against *ASA 8.4.2*. 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.

Prerequisites

Configure *Cisco Firewall* using the recommendations defined in the *CIS Cisco Firewall Benchmark v3.0.0* Level I or Level I and II profile.

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 Firewall* on ASA or ASA SM 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
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*
Justin Opatrny

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
Dan Didier, *NetSecureIA, Inc.*
Blake Frantz, *Center for Internet Security*
Michael Hamelin
Ashwin Kohli, *CCIE SEC & R&S*
Slava Kurenyshev
Andy McConnell, *Tripwire, Inc.*
Tim Muniz, *Tenable Network Security, Inc.*
Jason Nehrboss, *Computer Sciences Corporation*
Justin Opatrny
Sergev Pavlov
Vu Dao Quang
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

Description:
This benchmark for Cisco firewall appliances represents a prudent level of minimum due care. These settings:

- Can be easily understood and performed by system administrators with any level of security knowledge and experience.
- Are unlikely to cause an interruption of service to the operating system or the applications that run on it.

1.1 Routing

Description:
Configuration of routing on an Internet edge firewall should be done in such a manner as to prevent manipulation of network traffic and denial of service.

1.1.1 Require Static Routes for Internet Next Hop Gateway (Level 1, Scorable)

Description:
A static route should be configured between the firewall and the next hop Internet gateway to simplify configuration and prevent manipulation of the path to the Internet.

Rationale:
The next hop from the firewall to the Internet should be statically configured as it does not change often and represents an attack vector that could be used during a denial of service attack. Routing protocol can also be used to redirect traffic, allowing an attacker to hijack connections and compromise sensitive data.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure a default route to the internet next hop gateway router from the firewall.

```
hostname(config)#route if_name dest_ip mask gateway_ip [distance]
```

Audit:
Perform the following to determine if static default routes to the Internet are enabled:

```
hostname#show route
```

Default Value:
None

Scoring Status:
Scorable

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 Forbid Route Advertisements on Public Interfaces (Level 1, Scorable)

Description:
Routing protocol advertisements should be disabled on public interfaces to prevent an attack of the routing process itself.

1.1.2.1 OSPF (Level 1, Scorable)

Rationale:
Routing protocols will automatically create adjacencies if not controlled through authentication. Disabling the routing process on a statically configured public interface to reduce the threat of attack and protects the routing process of the firewall if used for internal networks to learn about the Internet default route.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure OSPF areas so that they do not include network addresses for Internet connections.

```
hostname(config)#router ospf process_id
hostname(config-router)#area area-id range ip-address mask [advertise |
not-advertise]
```

Audit:
Perform the following to determine if OSPF routing processes are enabled on Internet facing interfaces:

```
hostname#show ospf interface
```

Default Value:
None

Scoring Status:
Scorable

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 RIP (Level 1, Scorable)

Rationale:
Routing protocols will automatically create adjacencies if not controlled through authentication. Disabling the routing process on a statically configured public interface to

reduce the threat of attack and protects the routing process of the firewall if used for internal networks to learn about the Internet default route.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure RIP so that interfaces used to connect to the public interface are passive and do not advertise routes.

```
hostname(config)#router rip as-num
hostname(config-router)#network network_address
hostname(config-router)#passive-interface [default | if_name]
```

Audit:
Perform the following to determine if RIP routing processes are enabled on Internet facing interfaces and that route advertisements are disabled for the firewall with the passive interface command:

```
hostname#show running-config router rip
```

Default Value:
None

Scoring Status:
Scorable

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 EIGRP (Level 1, Scorable)

Rationale:
Routing protocols will automatically create adjacencies if not controlled through authentication. Disabling the routing process on a statically configured public interface to reduce the threat of attack and protects the routing process of the firewall if used for internal networks to learn about the Internet default route.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure EIGRP so that interfaces used to connect to the public interface are passive and do not advertise routes.

```
hostname(config)#router eigrp as-num
hostname(config-router)#network network_address
hostname(config-router)#passive-interface [default | if_name]
```

Audit:
Perform the following to determine if EIGRP routing processes are enabled on Internet facing interfaces and that route advertisements are disabled for the firewall with the passive interface command:

```
hostname#show running-config router eigrp
```

Default Value:
None

Scoring Status:
Scorable

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 Redistribute Static Default Route to internal routing protocols (Level 1, Scorable)

Description:
Verify that authentication, authorization and accounting (AAA) configuration uses required servers and protocols.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure designated security protocol, server, key and timeout used for authenticating users.

```
hostname(config)#aaa-server {server-tag} protocol { Kerberos | ldap |
nt | radius | sdi |tacacs+ }
hostname(config)#aaa-server {server-tag} host {aaa_server-ip} [key]
[timeout seconds]
```

Audit:
Perform the following to determine if AAA services are enabled:

```
hostname#show run aaa-server
```

Default Value:
The default value for `aaa-server` is disabled.

Scoring Status:
Scorable

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 Require Routing Protocol Authentication for Internal Routing

Description:
Routing protocols should be configured to use authentication in order to prevent unauthorized manipulation of network routing tables. If the Firewall is used to inject routes into the routing table, it must use authentication.

1.1.4.1 Require EIGRP Authentication for Internal Routes (Level 1, Scorable)

Description:
Verify enhanced interior gateway routing protocol (EIGRP) authentication is enabled, if routing protocol is used, where feasible.

Rationale:
Verifying routing update packets using neighbor authentication reduces the possibility of the device receiving false route updates that could potentially allow an attacker to corrupt route tables, compromise network availability, or redirect network traffic.

Warning:
If you configure the device for neighbor authentication, the neighbor device must be configured for neighbor authentication with compatible settings otherwise route update packets from the neighbor device will be rejected.

Remediation:
Configure EIGRP neighbor authentication where feasible.

```
hostname(config)#interface <interface_name>
hostname(config-if)#authentication mode eigrp as-num md5
hostname(config-if)#authentication key eigrp as-num key key-id key-id
```

Audit:
Perform the following to determine if the EIGRP authentication is enabled:

```
hostname#sh run int <interface>
```

Scoring Status:
Scorable

Default Value:

EIGRP authentication is disabled by default.

Additional References:

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

1.1.4.2 Require OSPF Authentication for Internal Routes (Level 1, Scorable)

Description:
Verify open shortest path first (OSPF) authentication is enabled, where feasible.

Rationale:
Verifying routing update packets using neighbor authentication reduces the possibility of the device receiving false route updates that could potentially allow an attacker to corrupt route tables, compromise network availability, or redirect network traffic.

Warning:
If you configure the device for neighbor authentication, the neighbor device must be configured for neighbor authentication with compatible settings otherwise route update packets from the neighbor device will be rejected.

Remediation:
Configure OSPF neighbor authentication where feasible.

```
hostname(config)#router ospf <ospf_process-id>
hostname(config-router)#area area-id authentication message-digest
```

Or

```
hostname(config)#interface <interface_name>
hostname(config-if)#ospf authentication [message-digest | null]
hostname(config-if)#ospf message-digest-key key_id md5 key
```

Audit:
Perform the following to determine if the OSPF authentication is enabled:

1. Verify message digest for OSPF areas are defined

```
hostname#sh run router ospf
```

2. Verify the appropriate md5 key and authentication is defined on the appropriate interface(s)

```
hostname#sh run int <interface>
```

Scoring Status:
Scorable

Default Value:
OSPF authentication is disabled by default.

Additional References:

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

1.1.4.3 Require RIPv2 Authentication for Internal Routes (Level 1, Scorable)

Description:
Verify routing information protocol (RIP) version two authentication is enabled, if routing protocol is used, where feasible.

Rationale:
Verifying routing update packets using neighbor authentication reduces the possibility of the device receiving false route updates that could potentially allow an attacker to corrupt route tables, compromise network availability, or redirect network traffic.

Warning:
If you configure the device for neighbor authentication, the neighbor device must be configured for neighbor authentication with compatible settings otherwise route update packets from the neighbor device will be rejected.

Remediation:
Configure RIPv2 neighbor authentication where feasible.

```
hostname(config)#interface <interface_name>
hostname(config-if)#rip authentication mode {text | md5}
hostname(config-if)#rip authentication key key key-id key-id
```

Audit:
Perform the following to determine if the RIPv2 authentication is enabled:

```
hostname#sh run int <interface>
```

Scoring Status:
Scorable

Default Value:
RIPv2 authentication is disabled by default.

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

1.2 Availability

Description:
Redundant hardware and ISP connections are commonly used to provide protection against hardware and network failures.

1.2.1 Require Failover Key (Level 1, Scorable)

Description:

Failover keys should be used to authenticate and encrypt failover information exchanges between to firewalls.

Rationale:
All information sent over the failover and stateful failover links is sent in clear text, which includes usernames, passwords, and any preshared keys used to establish VPN tunnels. In order to protect the confidentiality of this information a failover key should be used.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure a failover key on both firewalls.

```
hostname(config)#failover key password
```

Audit:
Perform the following command to determine that a failover key is configured:

```
hostname#show run failover
```

Default Value:
None

Scoring Status:
Scorable

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

1.3 Management

Description:
Management protocols should not be enabled on public facing network connections. All network connections made through the firewall should be logged.

1.3.1 Forbid SNMP (Level 1, Scorable)

Description:
SNMP should never be enabled on a public facing Internet connection to prevent community string guessing.

Rationale:
Attackers can use SNMP to view configuration settings and modify the configuration of the FW. Due to the lack of security features in SNMP v1 and v2 it is recommended that it be disabled on all public internet connections. While SNMP v3 supports authentication and encryption it should still be disabled to reduce the attack surface of the Firewall.

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable SNMP read access to the device.

```
hostname(config)#clear configure snmp-server
```

Audit:
Perform the following to determine if SNMP is configured, if the command returns values then SNMP is enabled:

```
hostname#show run snmp-server
```

Default Value:
SNMP is not enabled by default.

Scoring Status:
Scorable

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

1.3.2 Forbid Firewall Management on Public Interfaces (Level 1, Scorable)

Description:
The firewall can be managed through telnet, SSH, and SSL through the integrated device manager. These management tools should not be enabled on publicly facing internet connections.

Rationale:
In order to reduce the attack surface of the firewall, you should never allow direct Internet access to management facilities. It is recommended to configure the firewall to not respond to these ports and services.

Remediation:
Configure management access for an internal network interface or the dedicated management interface.

```
hostname(config)#management-access <interface_name>
```

Audit:
Perform the following to determine that management access is not enabled on a public facing interface:

```
hostname#sh run management-access
```

Scoring Status:
Scorable

Default Value:
None.

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

1.4 Network Address Translation

Description:
Network address translation (NAT) should be configured to prevent direct access from the internet to user and non-publicly available infrastructure devices.

Rationale:
Network address translations primary benefit is to provide oversubscription of limited publicly routable addresses for communication across the Internet. NAT also provides the ability to hide an internal network topology by translating internal addresses to public addresses. NAT prevents direct communications from the outside of the network to the inside without explicitly configuring address or port forwarding, which helps prevent attackers from connecting to internal user devices from outside the network.

1.4.1 Require NAT for User Devices to Access the Internet (Level 1, Scorable)

Description:
Configure NAT for internal network internet access.

Rationale:
Users should access the internet through NAT to hide internal topology and prevent direct access from the internet.

Remediation:
Configure NAT for all internal network segments where users need Internet access.

```
hostname(config)#object network <object_name>
hostname(config-network-object)#nat [(real_ifc,mapped_ifc)] dynamic
mapped_obj [pat-pool mapped_obj [round-robin]] [interface] [dns]
```

Audit:
Perform the following to determine if NAT is configured for user facing network segments:

```
hostname#sh nat
```

Scoring Status:
Scorable

Default Value:
NAT is disabled by default.

Additional References:
1. ASA 5500 Series Configuration Guide using the CLI 8.4

2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.2.0

1.5 Firewall Rules

Description:
Firewall rules should be constructed in a manner that allows for consistent policy enforcement and self-documentation. In addition connections that are denied based on policy should be logged to aid in the analysis of intrusion attempts.

Rationale:
Policy objects and groups allow the creation of logical structures for mapping security policy to firewall rules. These structures can simplify rule creation and aid in troubleshooting. All objects and groups should also include a description of their intent to ease readability of the rules for administrators to follow. Any rules that are constructed as a default deny all should be configured for logging to document suspicious behavior and source IP addresses.

1.5.1 Require Network Objects for Rule Construction (Level 1, Scorable)

Description:
Configure network objects to apply similar policies to a single host, network, or range of addresses.

Rationale:
Policies should be applied consistently to network devices and subnets.

Remediation:
Configure network objects for firewall rule creation.

```
hostname(config)#object network <object_name>
hostname(config-network-object)# {host ip_addr | subnet net_addr
net_mask | range ip_addr_1 ip_addr_2}
```

Audit:
Perform the following to determine if network objects are configured:

```
hostname#sh run | include object network
```

Scoring Status:
Scorable

Default Value:
None

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

1.5.2 Require Service Objects for Rule Construction (Level 1, Scorable)

Description:
Configure service objects for protocols and ports that will be used in rule creation.

Rationale:
Policies should be applied consistently to network devices and subnets.

Remediation:
Configure service objects for firewall rule creation.

```
hostname(config)#object network <object_name>
hostname(config-network-object)#service {protocol | icmp icmp-type |
icmp6 icmp6-type | {tcp | udp} [source operator port] [destination
operator port]}
```

Audit:
Perform the following to determine if service objects are configured:

```
hostname#sh run | include object service
```

Scoring Status:
Scorable

Default Value:
None

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

1.5.3 Require Network Object Groups for Rule Construction (Level 1, Scorable)

Description:
Network Object groups create combined policy constructs that can simplify rule creation by combining network objects into a logical grouping of networks and devices.

Rationale:
Firewall rules should be created to represent security policy efficiently and allow for rule reuse. Network Object groups can be created to map network services to logical zones and segments which makes it easier to troubleshoot and apply polices in a consistent manner.

Remediation:
Configure network object groups for ranges of addresses and hosts.

```
hostname(config)#object-group network grp_id
hostname(config-network)#network-object {object_name | host
ip_address | ip_address mask}
```

Audit:
Perform the following to determine if network object groups are used:

```
hostname#sh object-group network
```

Scoring Status:
Scorable

Default Value:
None

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

1.5.4 Require Network Object Group Descriptions (Level 1, Scorable)

Description:
Configure descriptions for objects groups to aid in troubleshooting and auditing the purpose of the rules.

Rationale:
Documenting the function of an object group can provide a self-documenting feature that can help auditors and administrators better understand the intent and purpose of complex rules.

Remediation:
Configure descriptions of object groups.

```
hostname(config)#object-group network grp_id
hostname(config-network)#description text
```

Audit:
Perform the following to determine if descriptions are present for network object groups:

```
hostname#sh object-group network
```

Scoring Status:
Scorable

Default Value:
None

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

1.5.5 Require Service Object Groups for Rule Construction (Level 1, Scorable)

Description:
Service Object groups create combined policy constructs that can simplify rule creation by combining objects into a logical group of ports and protocols.

Rationale:
Firewall rules should be created to represent security policy efficiently and allow for rule reuse. Service object groups can be created to map network services to logical zones and segments which makes it easier to troubleshoot and apply polices in a consistent manner.

Remediation:
Configure service object groups.

```
hostname(config)#object-group service I {tcp | udp | tcp-udp}
hostname(config-service)#port-object {eq port | range begin_port
end_port}
```

Audit:
Perform the following to determine if service object groups are used:

```
hostname#sh object-group service
```

Scoring Status:
Scorable

Default Value:
None.

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

1.5.6 Require Service Object Group Descriptions (Level 1, Scorable)

Description:
Configure descriptions for objects groups to aid in troubleshooting and auditing the purpose of the rules.

Rationale:
Documenting the function of an object group can provide a self-documenting feature that can help auditors and administrators better understand the intent and purpose of complex rules.

Remediation:
Configure descriptions of object groups.

```
hostname(config)#object-group service grp_id {tcp | udp | tcp-udp}
hostname(config-service)#description text
```

Audit:
Perform the following to determine if descriptions are present for service object groups:

```
hostname#sh object-group service
```

Scoring Status:

Scorable

Default Value:
None

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

1.5.7 Require Logging for Default Deny Rule (Level 1, Scorable)

Description:
Traffic that is denied due to firewall rules should be logged to provide a record of potential misuse.

Rationale:
Firewall access lists have an implicit deny all entry at the end of the access list to block traffic that is not permitted. In order to log this blocked traffic, the firewall must be configured with an access control entry that utilizes the log keyword.

Remediation:
Configure a default deny all entry with the log key word on Internet segments.

```
hostname(config)#access-list access_list_name deny ip any any [log
[[level] [interval secs] | disable | default]]
```

Audit:
Perform the following to determine if logging is enabled:

```
Hostname# sh run | include access-list
```

Scoring Status:
Scorable

Default Value:
Default deny all logging is disabled.

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

1.6 Threat Detection

Description:
Threat detection techniques should be configured in order to block known malicious traffic and network addresses.

Rationale:
Known malicious traffic and network address ranges can be used to block access to malware sites without having to inspect every packet on the network. This technology

reduces risk through a process that is analogous to listing all of the bad neighborhoods in town and simply not going into them.

1.6.1 Require Botnet Traffic Filter (Level 2, Scorable)

Description:
Botnet Traffic filter is a dynamically updated database that lists know malware sites and denies client network connections to these parts of the internet.

Rationale:
A blacklist of know malware sites is useful in preventing the spread of malware and identifying infected machines attempting "phone home" to command and control mechanisms used in botnets.

1.6.1.1 Require Dynamic Filter Updates (Level 2, Scorable)

Description:
Configure Dynamic Filter update and set the firewall to use the new database of knows malicious sites.

Rationale:
The botnet database is a subscription service that is updated and maintained by Cisco. The latest versions must be downloaded to the firewall to provide protection from identified botnet and malware hosting sites.

Remediation:
Configure the firewall to update and use the botnet database.

```
hostname(config)#dynamic-filter updater-client enable
hostname(config)#dynamic-filter use-database
```

Audit:
Perform the following to determine if service objects are configured:

```
hostname#sh run | include dynamic-filter
```

Scoring Status:
Scorable

Default Value:
None

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

1.6.1.2 Require DNS Snooping (Level 2, Scorable)

Description:
Configure DNS snooping for botnet traffic filtering.

Rationale:
DNS snooping is used to identify device requests for malicious websites and servers.

Remediation:
Configure DNS Snooping and apply it to internal interfaces.

```
hostname(config)#class-map name
hostname(config-cmap)#match port udp eq domain
hostname(config)#policy-map name
hostname(config-pmap)#class name
hostname(config-pmap-c)#inspect dns [map_name] dynamic-filter-snoop
hostname(config)#service-policy policymap_name interface interface_name
```

Audit:
The following command will show if DNS snooping is configured and monitoring DNS address requests:

```
hostname#show dynamic-filter dns-snoop [detail]
```

Scoring Status:
Scorable

Default Value:
None

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

1.6.1.3 Require Botnet Traffic Filter (Level 2, Scorable)

Description:
Configure service objects for protocols and ports that will be used in rule creation.

Rationale:
Policies should be applied consistently to network devices and subnets.

Remediation:
Configure service objects for firewall rule creation.

```
hostname(config)#access-list access_list_name extended {deny | permit}
protocol source_address mask [operator port] dest_address mask
[operator port]
hostname(config)#dynamic-filter enable [interface name][classify-list
access_list]
hostname(config)#dynamic-filter drop blacklist [interface name] [action
classify-list subset_access_list] [threat-level {eq level | range min
max}]
hostname(config)#dynamic-filter ambiguous-is-black
```

Audit:

Perform the following to determine if Botnet filtering is configured:

```
hostname#sh run | include dynamic-filter
```

Scoring Status:
Scorable

Default Value:
None

Additional References:

1. ASA 5500 Series Configuration Guide using the CLI 8.4
2. 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
December 6, 2011	1.0.0	Public Release