硬化思科ASA防火墙的思科指南

目录

简介

本文包含信息帮助您巩固思科ASA设备，强化您的网络整体安全。本文在4个部分被构造

管理层面硬化-这应用对所有ASA涉及的Management/To方框流量类似SNMP， SSH等。
保护的设置-我们能停止填充运行配置的等密码等的命令
记录日志和监听-这适用于与注册ASA涉及的任何设置。
通过流量-这适用于通过ASA的流量。

通常，本文档对安全功能的介绍将提供足够详细的信息，以便于您配置该功能。但是，在未能提供详细信息的情况下，我们会对该功能进行说明，以便于您评估是否需要对该功能引起额外的关注。本文档将在可能和适当的地方提供一些在实施后将有助于保护网络安全的建议。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ASA5500-X 9.4(1)及以后。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置可能也与Cisco ASA 5500-X系列安全工具软件版本9.x一起使用。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

确保运行安全

确保网络运行安全是一个非常重要的主题。虽然大多数本文专用于思科ASA设备的安全的配置，单独配置完全不获取网络。网络上使用的运行过程与底层设备的配置一样，在很大程度上影响着网络的安全。

这些主题中包含一些建议您实施的操作建议。这些主题主要着眼于网络运行的特定重要方面，因此并不全面。

监视 Cisco 安全建议及响应

Cisco 产品安全事件响应小组 (PSIRT) 针对 Cisco 产品中与安全相关的问题，创建并维护通常称为《PSIRT 建议》的出版物。可使用“Cisco 安全响应”这一方法来传达严重程度较低的问题。安全建议和答复是可用的在PSIRT。

在 Cisco 安全漏洞策略中可以找到有关这些通信手段的其他信息。

为维护网络安全，您需要了解已发布的 Cisco 安全建议和响应。您首先需要了解有关漏洞的知识，然后才能评估漏洞可能对网络造成的威胁。要完成此评估过程，请参阅安全漏洞通告风险分类以获取相应的帮助。

利用身份验证、授权和记账

验证、授权和统计(AAA)框架是重要巩固网络设备。AAA 框架提供针对管理会话的身份验证功能，还可以将用户限制为只能执行特定的、管理员定义的命令，并记录所有用户输入的全部命令。请参阅本文的认证、授权和记帐部分关于如何有效利用AAA的更多信息。

集中处理日志收集和监视

为了获取关于存在的知识，涌现，并且有历史的事件与安全事件涉及，您的组织必须有事件日志和相关性的一个统一的策略。此策略必须利用来自所有网络设备的日志记录，并使用预封装的可自定义关联功能。

实施集中式日志记录后，您必须开发一个用于进行日志分析和事件跟踪的结构化方法。基于您组织的需要，此方法的范围可以介于对日志数据的简单复查和基于规则的高级分析之间。

尽可能使用安全协议

许多协议用于传送敏感的网络管理数据。您必须尽可能使用安全协议。一种安全协议选择包括使用 SSH（而不使用 Telnet），以便对身份验证数据和管理信息进行加密。此外，在复制配置数据时，您必须使用安全的文件传输协议。例如，使用安全复制协议 (SCP) 代替 FTP 或 TFTP。

使用 NetFlow 获得数据流可见性

使用 NetFlow 可以监视网络中的数据流。尽管最初用于将数据流信息导出到网络管理应用程序中

，但 NetFlow 也可用于在路由器上显示数据流信息。使用此功能可以实时查看经过网络的数据流。不论数据流信息是否导出到远程收集器，建议您针对 NetFlow 配置网络设备，以便可以在需要时反应性地使用 NetFlow。

配置管理

配置管理是用于建议、审查、批准并部署配置更改的过程。在思科ASA设备配置的上下文内，配置管理的两个另外的方面是关键：配置存档和安全。

您可以使用配置存档来回滚对网络设备所做的更改。在有关安全的上下文中，配置存档还可用于确定已做出的安全更改，以及发生这些更改的时间。与 AAA 日志数据相结合，此信息可在对网络设备进行安全审计时提供帮助。

思科ASA设备的配置包含许多敏感详细信息。用户名、口令和访问控制列表的内容都属于此类型的信息。您使用为了归档思科ASA设备配置的信息库需要被巩固。以不安全的方式访问这些信息可能会破坏整个网络的安全。

管理平面

管理平面包含用于实现网络管理目标的功能。这包括使用SSH的交互管理会话，以及统计信息采集与SNMP或Netflow。考虑网络设备的安全时，保护管理平面非常重要。如果安全事件能够破坏管理平面的功能，您可能将无法恢复网络或使网络变得稳定。

硬化管理层面

管理平面用于访问、配置和管理设备，并用于监视该设备的运行情况及部署该设备的网络。管理平面是接收和发送用于运行这些功能的数据流的平面。以下为管理平面使用的协议列表：

- 简单网络管理协议 (SNMP)
- Secure Shell 协议 （SSH）
- 文件传输协议
- 简单文件传输协议 (TFTP)
- 安全复制协议 (SCP)
- TACACS+
- RADIUS
- Netflow
- 网络时间协议 (NTP)
- Syslog
- ICMP
- SMB

注意：启用，因为它是纯文本， TELNET没有推荐。

密码管理

口令控制对资源或设备的访问。这通过定义用于对请求进行身份验证的口令或加密口令来实现。收到针对资源或设备的访问请求时，将对该请求进行质询，以便验证口令和身份，然后再根据质询结果授予、拒绝授予或限制访问权限。作为一项安全最佳实践，口令必须使用 TACACS+ 或 RADIUS 身份验证服务器进行管理。然而，请注意在TACACS+的失败或RADIUS服务情形下，特许访问的一

本地配置的口令还是必要。设备的配置中也可能存在其他口令信息，如 NTP 密钥、SNMP 社区字符串或路由协议密钥。

ASA使用消息摘要5 (MD5)密码散列。此算法曾受到相当多的公开检验，并被认为是不可逆的。但是，此算法容易受到字典攻击。在字典攻击中，攻击者尝试字典或其他一组候选口令中的每一个词，希望找到匹配项。因此，必须安全地存储配置文件，并仅与受信任的个人共享该文件。

Enable (event) HTTP服务

要使用ASDM，您需要启用HTTPS服务器，并且允许对ASA的HTTPS连接。安全工具允许最多每上下文5个并发ASDM实例，若有，有最多的在所有上下文之间的32个ASDM实例。配置ASDM访问使用：

```
http server enable <port>
```

允许在ACL列表必要仅的IP的。允许一宽访问是错误的实践。

```
http 0.0.0.0 0.0.0.0 <interface>
```

配置ASDM访问控制：

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

开始用ASA软件版本9.1(2),8.4(4.1)， ASA现在支持以下短暂Diffie-Hellman (DHE) SSL密码器套件。

DHE-AES128-SHA1
DHE-AES256-SHA1

这些密码器套件在**RFC 3268**指定，传输层安全的(TLS)高级加密标准(AES) Ciphersuites。

当支持由客户端， DHE是首选的密码器，因为提供优秀的转发保密性。请参阅以下限制：

SSL 3.0连接不支持DHE，因此请确保也启用SSL服务器的TLS 1.0。

```
// Set server version ASA(config)# ssl server-version tlsv1 sslv3
// Set client version ASA(config) # ssl client-version any
```

一些普遍的应用程序不支持DHE，因此请包括至少其他一个Ssl encryption方法保证可以使用密码器套件普通对两个SSL客户端和服务器。一些客户端可能不支持DHE，包括AnyConnect 2.5和3.0，Cisco Secure Desktop和Internet Explorer 9.0。

ASA有在作为下面启用的按顺序密码器之下默认情况下。

```
ASA(config)#ssl encryption rc4-sha1 dhe-aes128-sha1 dhe-aes256-sha1 aes128-sha1 aes256-sha1
3des-sha1
```

其中任一ssl服务器版本(默认)

默认情况下ASA使用在每辆重新启动更改的一临时自签名证书。如果寻找单个证书，您能跟随下面的链路生成一永久性自签名证书。

现在ASA支持TLS从软件版本9.3.1for的版本1.2 startig保护ASDM、无客户端SSVPN和AnyConnect的VPN消息传输。 以下命令介绍或被修改的命令：**ssl客户端版本**， **ssl服务器版本**，**ssl密码器**， **ssl托拉斯点**， **ssl DH组**，**显示ssl**，**显示ssl密码器**，**显示vpn-sessiondb**

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

启用 SSH

ASA允许对ASA的SSH连接管理目的。ASA允许最多每上下文5并发SSH连接，若有，有最多的100连接分开在所有上下文之间。

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

默认密钥对类型是一般密钥。默认模数大小是1024。相当数量存储的密钥对NVRAM空间根据ASA平台变化。如果生成超过30密钥对，您可以达到限制。ASA5580， 5585，或以上平台只支持4096位RSA密钥。

取消指示的类型的密钥对(rsa或dsa)

```
crypto key zeroize { rsa | dsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

配置远程设备访问的SSH ：

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

要限制ASA接受的SSH版本，请使用version命令的SSH在全局配置模式。要限制ASA只使用版本2可以是在命令之下穿上wusing。

```
ASA(config)#ssh version 2
```

使用Diffie-Hellman (DH) Group1或DH组14密钥交换方法，要交换密钥，请使用SSH密钥交换in命令全局配置模式。从9.1(2) SSH的ASA支持dh-group14-sha1开始

```
ASA(config)#ssh key-exchange dh-group14-sha1
```

配置登录会话的超时

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

密码管理

口令控制对资源或设备的访问。这通过定义用于对请求进行身份验证的口令或加密口令来实现。收到针对资源或设备的访问请求时，将对该请求进行质询，以便验证口令和身份，然后再根据质询结果授予、拒绝授予或限制访问权限。作为一项安全最佳实践，口令必须使用 TACACS+ 或 RADIUS 身份验证服务器进行管理。然而，请注意在TACACS+的失败或RADIUS服务情形下，特许访问的一本地配置的口令还是必要。设备的配置中也可能存在其他口令信息，如 NTP 密钥、SNMP 社区字符串或路由协议密钥。

配置本地用户和加密密码

```
username <local_username> password <local_password> encrypted
```

配置特权密码

```
enable password <enable_password> encrypted
```

配置特权模式的AAA认证

```
ASA(config)#aaa authentication enable console LOCAL
```

验证、授权和记帐

验证、授权和统计(AAA)框架是关键为了获取对网络设备的交互式访问。AAA框架提供可以被剪裁根据网络的需要的一个高度可配置环境。

TACACS+ 身份验证

TACACS+是ASA能使用管理用户验证一个远程AAA服务器的认证协议。这些管理用户能通过SSH、HTTPS、telnet或者HTTP访问ASA设备。

TACACS+ 身份验证（更常被称为 AAA 验证）使每个网络管理员能够使用单个用户帐户。当您不取决于单个共享密码时，网络的安全改善，并且您的责任被加强。

RADIUS是协议相似在目的与TACACS+;然而，它只加密在间网络被发送的密码。相反，TACACS+加密整个TCP有效载荷，包括两个用户名和密码。因此，当 AAA 服务器支持 TACACS+ 时，应使用 TACACS+，而不使用 RADIUS。有关比较这两种协议的详细信息，请参阅比较 TACACS+ 和 RADIUS。

TACACS+认证在有配置的一个思科ASA设备可以启用类似于此示例：

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

ASA镜像签字和验证

使用数字签名，从软件版本9.3.1 ASA开始镜像当前签字。在ASA是启动后，数字签名验证。

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done! Embedded Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e Computed Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e CCO Hash SHA-512:
1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
```

```
c99f49f70354715441385e0b96e4bd3e861d18fb30433d52e12b15b501fa790f36d0ea0 Signature Verified
ASA(config)# verify /signature running Requesting verify signature of the running image...
Starting image verification Hash Computation: 100% Done! Computed Hash SHA2:
2fbb0f62b5fbc61b081acfca76bddbb2 26ce7a5fb4b424e5e21636c6c8a7d665
1e688834203dfb7ffa6eaefc7fdf9d3d 1d0a063a20539baba72c2526ca37771c Get key records from key
storage: PrimaryASA, key_store_type: 6 Embedded Hash SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
26ce7a5fb4b424e5e21636c6c8a7d665 1e688834203dfb7ffa6eaefc7fdf9d3d
1d0a063a20539baba72c2526ca37771c Returned. rc: 0, status: 1 The digital signature of the running
image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
Signer Information
Common Name : abraxas
Organization Unit : ASAv
Organization Name : CiscoSystems
Certificate Serial Number : 550DBBD5
Hash Algorithm : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version : A
```

配置时钟时间区域

```
clock timezone GMT <hours offset>
```

配置NTP

网络时间协议 (NTP) 并不是一种特别危险的服务，但任何不必要的服务都可能代表攻击矢量。如果使用 NTP，则必须明确配置受信任的时间源并使用适当的验证。为了实现 syslog 目的（例如在对潜在的攻击进行取证调查期间），并且为了在依靠证书进行第 1 阶段验证时成功建立 VPN 连接，需要使用准确而可靠的时间。

- **NTP时间区域**-当您配置NTP时，时间区域需要配置，以便时间戳可以准确地关联。通常有配置设备的时间区域的两个途径在网络以一全局在线状态。一种方法是使用协调世界时 (UTC)（以前称为格林威治标准时间 (GMT)）配置所有网络设备。另一种方法是使用本地时区配置网络设备。

```
ntp server ip_address [ key key_id ] [ source interface_name ] [ prefer ]
```

- **NTP认证**-如果配置NTP认证，提供保证NTP消息被交换在委托NTP对等体之间。启用认证使用ntp authenticate命令，设置此服务器的信任键ID。如果启用认证， ASA只传达与Ntp server，如果在数据包使用正确信任键。对与Ntp server的启用认证，请使用ntp authenticate命令在全局配置模式。

```
ASA(config)#ntp authenticate
```

DHCP服务器服务(如果不使用)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

注意：ASA不支持CDP。

访问列表控制面板

对这方框管理数据流的访问控制规则(定义由这样命令象http、SSH或者telnet)比访问列表有更高的优先应用与控制面板选项。所以，这样允许的管理数据流将允许进来，即使明确地拒绝由对这方框访问列表。

```
access-list <name> in interface <Interface_name> control-plane
```

从ASA

这是可以用于复制/转移文件到ASA的协议。

明文：

- FTP
- HTTP
- TFTP
- SMB

安全：

- HTTPS
- SCP (安全的复制客户端)从9.1(5)开始， ASA转接文件的支持SCP客户端到/从SCP服务器。

通过流量

TCP序列号随机化

每TCP连接有两ISNs ：一个由客户端生成，另一个由服务器生成。ASA随机化通过在入站和出站方向的TCP SYN的ISN。

随机化已保护主机的ISN防止一名攻击者predecting新连接的下个ISN和潜在劫持个新会话。

您可以根据需要禁用 TCP 初始序列号随机化。例如：

- 如果另一个在线防火墙也执行初始序列号随机化，则这两个防火墙不必都执行此操作，尽管此操作不影响数据流。
- 如果通过ASA使用EBGP多跳，并且eBGP对等体使用MD5。随机化中断MD5校验和。
- 如果我们使用要求ASA不随机化连接序号的一个WAAS设备。

TTL减少量

默认情况下，不减少在IP报头的TTL由于哪个ASA没出现作为路由器跳，当执行Traceroute时。

dnsguard

强制执行每查询一DNS答复。使用in命令全局配置模式，它可以启用。

```
ASA(config)#dns-guard
```

配置片段链分段检查

要提供信息包分段的另外的管理和改进兼容性与NFS，请使用fragment命令在全局配置模式。

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

配置协议检测

检查引擎为在用户数据数据包嵌入IP寻址信息或在动态地已分配端口的开放次信道的服务要求。这些协议要求ASA执行深度信息包检验而不是通过数据包到快速路径。结果，检查引擎能影响整体吞吐量。为关于应用层协议检查的详细信息请参考ASA 9.4设置指南。

在ASA的检查可以是启用的使用在命令之下

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

默认情况下ASA有“”启用的global_policy全局。

配置单播反向路径转发

```
ip verify reverse-path interface <interface_name>
```

当流量被撤销由于RPF检查时，在ASA增量的下面的“请显示asp丢弃”计数器。

```
ASA(config)# show asp drop

Frame drop:
 Invalid TCP Length (invalid-tcp-hdr-length)                    21
   Reverse-path verify failed (rpf-violated)                     90

// Check Reverse path statistics

ASA(config)# sh ip verify statistics
 interface inside: 11 unicast rpf drops
interface outside: 79 unicast rpf drops
```

威胁检测

在他们到达内部网络基础设施前，威胁检测提供防火墙管理员必要的工具识别，了解和终止攻击。为了执行如此，功能依靠一定数量不同的触发和统计信息，在这些部分的更详细的资料描述。

请参考ASA威胁检测功能和配置详细说明的在威胁检测在ASA。

僵尸网络过滤器

僵尸网络数据流过滤器监视器域名服务器(DNS)请求和答复在内部DNS客户端和外部DNS服务器之间。当DNS答复处理时，域关联与答复根据已知有恶意的域数据库核对。如果有匹配，对IP地址的任何另外流量现在DNS答复阻塞。

恶意软件是在一台不知道的主机安装的恶意的软件。恶意软件(密码、信用卡号、关键冲程或者尝试网络活动例如发送私有数据的所有权数据)可以由僵尸网络数据流过滤器检测，当恶意软件开始对已知坏IP地址时的一连接。僵尸网络数据流过滤器根据一个动态数据库已知坏域名和IP地址检查流入和输出连接(*黑名单*)，然后日志或者阻塞所有可疑活动。

您能用列入黑名单的地址您选择也补充思科动态数据库通过添加他们到一个静态黑名单;如果动态数据库包括您认为的列入黑名单的地址不如果列入黑名单，您能手工输入他们到一静态*whitelist*。Whitelisted地址仍然生成系统消息，但是，因为您只瞄准黑名单系统消息，他们信息性。为详细信息请参考配置僵尸网络数据流过滤器。

未连接的子网的ARP缓存新增内容

默认情况下ASA不响应对非直接地连接的子网IP地址的ARP。如果有不属于ASA接口的相同子网IP在ASA的NAT IP，我们将必须启用“arp permitnonconnected”在ASA到proxy-arp NATted IP的。

```
arp permit-nonconnected
```

总是推荐有在上行和下行设备的正确路由NAT的能工作，无需启用上述命令。

记录日志和监听

配置SNMP

此部分突出显示能使用为了获取SNMP部署在ASA设备内的几个方法。非常重要的是SNMP适当地获取为了保护此数据传输网络数据和网络设备的机密性、完整性和可用性。SNMP 可为您提供大量有关网络设备运行状况的信息。应该从要有效利用此数据为了进行攻击网络的有恶意的用户保护此信息。

SNMP 社区字符串

社区字符串是应用到ASA设备限制访问，只读和读写访问的密码，对在设备的SNMP数据。和所有口令一样，这些社区字符串应经过仔细选择，以确保它们具有保密作用。社区字符串应根据网络安全策略定期进行更改。例如，在网络管理员更换职位或离开公司时，应更改社区字符串。

Enable (event) SNMP读访问：

```
snmp-server host <interface_name> <remote_ip_address>
```

Enable (event) SNMP陷阱

```
snmp-server enable traps all
```

配置Syslog

它建议发送记录信息到远程系统日志服务器。这使成为可能更加有效关联和审计网络和安全事件在网络设备间。请注意，syslog 消息通过 UDP 以明文形式传输，这种传输方式并不可靠。例如为此，网络能管理数据流应该扩展的所有保护(加密或带外访问)为了包括Syslog流量。日志可以cofnigured发送到从ASA的以下目的地：

- ASDM
- 缓冲区
- 闪存
- 发送邮件
- FTP服务器
- SNMP服务器作为陷阱
- 系统日志服务器

配置控制台记录严重级别

```
logging console critical
```

TCP基于Syslog也是可用的。所有系统日志可以发送到系统日志服务器在明文或在已加密在TCP的情况下。

明文

日志主机interface_name syslog_ip [TCP端口

已加密

日志主机*interface_name syslog_ip* [*TCP端口*][secure]

如果TCP连接不可能用系统日志服务器建立，所有新连接将拒绝。您可以通过输入“**记录日志permithostdown**”命令更改此默认行为。

配置在日志消息的时间戳

配置日志记录时间戳可帮助您关联各个网络设备上的事件。必须实施正确且一致的日志记录时间戳配置，以确保能够关联日志记录数据。

```
logging timestamp
```

对于另外相关的信息对Syslog请参考ASA Syslog配置示例。

配置Netflow

有时，特别是在事件响应或网络性能不佳的时候，您可能需要迅速标识和回溯网络数据流。使用 NetFlow 可以看到网络上的所有数据流。此外，NetFlow 还可以与能够提供长期趋势和自动分析的收集器一起实施。

Cisco ASA支持Netflow版本9服务。NSEL的ASA和ASASM实施提供一有状态的，跟踪导出仅那些记录指示在流的重大活动的方法的Ip流。在有状态的流跟踪，被跟踪的流通过一系列的状态变换。NSEL事件用于导出关于流状态的数据和由引起状态变换的事件触发。

欲知Netflow的更多信息在ASA的请参考思科ASA NetFlow实施指南：

保护的设置

在ASA的镜像验证

从9.1(2)和8.4(4.1)开始， SHA-512镜像完整性检查的支持被添加了。要验证文件的校验和，请使用verify命令在特权EXEC模式。

计算并且显示指定的软件镜像的MD5值。比较与值联机的此值在此镜像的Cisco.com。

```
verify [ /md5 path ] [ md5-value ]
```

在设置的密码

所有密码和密钥加密或被弄暗淡。“show running-config”不显示实际密码。

这样备份不可能用于备份/恢复在ASA。为恢复使用的备份目的whould执行使用命令“更多system: running-config”。使用一个重要的通行证惯用语，ASA设置密码可以加密。为详细信息请参考密码加密。

服务口令恢复

禁用此将禁用密码恢复机制并且禁用对ROMMON的访问。恢复唯一的平均值从丢失的或忘记的密码将是为了ROMMON能清除所有文件系统包括配置文件和镜像。您应该做备份您的配置和有恢复的机制从ROMMON line命令的镜像。

故障排除

没有本文的故障排除部分。