在Cisco VPN 3000集中器和路由器之间的LAN到LAN IPSec隧道有AES的配置示例的

目录

简介

本文显示如何配置在Cisco VPN 3000集中器和一个Cisco路由器之间的一个IPSec隧道有Advance Encryption Standard (AES)的作为加密算法。

AES是美国标准技术研究所(NIST)新发布的联邦信息处理标准(FIPS)，将用作加密方法。此标准指定替换数据加密标准(DES)作为IPsec和Internet Key Exchange (IKE)的一次保密性转换的AES对称加密算法。AES有三个不同的密钥长度、一个128位密钥(默认值)，一个192位密钥和一个256位密钥。在Cisco IOS的AES功能添加新的加密标准AES的支持，同密码链块(CBC)模式，到IPsec。

参考NIST计算机安全资源中心站点 关于AES的更多信息。

在Cisco VPN 3000集中器和PIX防火墙配置示例之间的参考的LAN到LAN IPSec隧道关于在VPN 3000集中器和PIX防火墙之间的LAN到LAN隧道配置的更多信息。

在PIX 7.x和VPN 3000集中器配置示例之间的参考的IPSec隧道欲知更多信息，当PIX有软件版本7.1。

先决条件

要求

本文要求IPSec协议基本的了解。要了解有关 IPsec 的详细信息，请参阅 IPsec 加密简介。

尝试进行此配置之前，请确保满足以下要求：

- **路由器需求**- AES功能在Cisco IOS软件版本12.2(13)T介绍。为了启用AES，您的路由器必须支持IPsec和运行IOS镜像以"k9"长密钥("k9"子系统)。**注意：** 支持AES的硬件也可在Cisco 2600XM、2691、3725和3745 AES加速VPN模块上使用。此功能没有配置暗示，并且如果两个都可用，硬件模块自动地选择。
- **VPN集中器需求**- AES功能的软件支持在版本3.6介绍。新的增强版提供硬件支持，可扩展加密处理器(SEP-E)。此功能没有配置暗示。**注意：** 在Cisco VPN 3000集中器版本3.6.3中，由于Cisco Bug ID CSCdy88797，隧道不与AES协商 (只限于注册用户)。这从版本3.6.4被解决了。**注意：** Cisco VPN 3000集中器使用SEP或SEP-E模块，不是两个。请勿安装两个在同一个设备。如果您将SEP-E模块安装在包含一个SEP模块的VPN集中器上，那么VPN集中器就禁用SEP模块，只使用SEP-E模块。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有Cisco IOS软件版本12.3(5)的Cisco 3600系列路由器
- Cisco VPN 3060集中器用软件版本4.0.3

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- IPSec路由器
- VPN 集中器

ipsec_router配置

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
```

```
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

注意： 虽然ACL语法不可更改，含义为加密ACL是有些不同的。在加密ACL， **permit**指定匹配数据包的那应该加密，而请**拒绝**指定匹配数据包的那不需要加密。

配置 VPN 集中器

VPN集中器在他们的出厂设置中没有预编程序设置IP地址。您必须使用控制台端口配置基于菜单的命令行界面(CLI)的初始配置。有关如何通过控制台进行配置的信息，请参阅通过控制台配置 VPN 集中器。

在Ethernet 1的IP地址以后(私有)接口配置，其余可以配置或者使用CLI或通过浏览器接口。浏览器界面支持 HTTP 和使用安全套接字层 (SSL) 的 HTTP。

以下参数通过控制台进行配置：

- **时间/日期**-正确时间和日期是非常重要。他们帮助保证记录和记帐条目是准确的，并且系统能创建一个有效安全证书。
- **Ethernet 1 (私有)接口**- IP地址和掩码(从我们的网络拓扑172.16.1.1/24)。

这时， VPN集中器通过从网络内部的一个HTML浏览器是可取得。欲了解在CLI模式下配置VPN集中器的信息，使用CLI参见快速配置。

1. 键入专用接口的IP地址从Web浏览器的启用GUI界面。点击**保存必要的**图标保存对内存的更改。出厂默认设置用户名和密码是“区分大小写的admin”。
2. 在您启动GUI后，请选择**Configuration > Interfaces > Ethernet 2 (公共)**配置Ethernet2接口。
3. 选择**Configuration > System** > IP Routing > Default Gateways配置默认(互联网)网关和通道默认(里面)网关IPsec的能到达其他子网在私有网络。在此方案中，只有在网络内部的一子网联机。
4. 选择**Configuration > Policy Management > Traffic Management > Network Lists** >Add建立定义流量的网络列表将加密。在列表提及的网络是可及的对远程网络。在列表显示的网络下面是本地网络。当您点击**Generate Local List时，**您能通过RIP自动地也生成本地网络列表。
5. 在此列表的网络是远程网络并且需要手工配置。为了执行此，请进入网络/通配符每可及的子

网的。当完成，这些是两张网络列表：

6. 选择**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add**并且定义LAN-to-LAN隧道。此窗口有三个部分。上面的部分是网络信息，而下面的两部分是本地和远程网络列表。在网络信息信息部分，请选择AES加密，认证类型， IKE建议，并且键入预先共享密钥。在底下部分，请指向您已经创建，各自本地和远程列表的网络列表。
7. 在您单击后请**添加**，如果您的连接正确，您提交与IPSec LAN-to-LAN-Add-Done窗口。此窗口提交隧道配置信息的总结。它自动地也配置组名， SA命名和过滤器名称。您在此表里能编辑所有参数。这时IPSec LAN到LAN隧道设置，并且您能开始工作。如果，由于某种原因，通道不工作，您能检查误配置。
8. 当您选择**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN时，**您能以前查看或修改创建的LAN对LAN IPSec参数。因为通道和远程终端的公共接口的名称是30.30.30.1根据方案，此图形显示“测验”。
9. 通常，如果您的IKE建议在Inactive Proposals列表，您的通道也许不出来。选择**Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**配置活动IKE建议。如果您的IKE建议在“非激活建议”列出您能启用它，当您选择IKE建议并且点击**激活**按钮时。在此图形选定建议"IKE-AES256-SHA"在有效建议列表。
10. 如果SA参数正确，请选择**Configuration > Policy Management > Traffic Management > Security Associations**验证。
11. 点击SA名称(在这种情况下， **L2L ：测验**)，然后单击**修改**验证SAS。如果其中任一个参数不配比与远端对等体配置，可以更改此处。

验证

验证路由器配置

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。状态QM_IDLE表示SA保持已验证与其对等体，并且可以用于随后的快速模式交换。它在一淡静状态。`ipsec_router#`**`show crypto isakmp sa`**

```
dst             src             state    conn-id   slot

20.20.20.1      30.30.30.1      QM_IDLE        1      0
```

- **show crypto ipsec sa** - 显示当前 SA 使用的设置。检查对等 IP 地址、本地和远程端都可访问的网络，以及所使用的转换集。有两个 ESP SA，每个方向一个。因为AH使用转换集，它是空的。`ipsec_router#`**`show crypto ipsec sa`**

```
interface: Ethernet1/0

       Crypto map tag: vpn, local addr. 30.30.30.1

       protected vrf:

        local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

       remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

       current_peer: 20.20.20.1:500
```

```
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145
 #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 6, #recv errors 0
 local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1
 path mtu 1500, media mtu 1500
 current outbound spi: 54FA9805
inbound esp sas:
spi: 0x4091292(67703442)
 transform: esp-256-aes esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
 sa timing: remaining key lifetime (k/sec): (4471883/28110)
 IV size: 16 bytes
 replay detection support: Y
inbound ah sas:
inbound pcp sas:
 outbound esp sas:
spi: 0x54FA9805(1425709061)
 transform: esp-256-aes esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
 sa timing: remaining key lifetime (k/sec): (4471883/28110)
 IV size: 16 bytes
 replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

- **show crypto engine connections active** —显示所有加密引擎的当前活动加密的会话连接。每连接ID是唯一。加密和解密信息包的数量在前二列中显示。`ipsec_router#`**`show crypto engine connections active`**

```
  ID      Interface     IP-Address    State    Algorithm          Encrypt Decrypt

   1      Ethernet1/0   30.30.30.1    set      HMAC_SHA+AES_256_C       0       0

2000      Ethernet1/0   30.30.30.1    set      HMAC_MD5+AES_256_C       0      19

2001      Ethernet1/0   30.30.30.1    set      HMAC_MD5+AES_256_C      19       0
```

验证VPN集中器配置

完成这些步骤验证VPN集中器配置。

1. 当您选择在VPN集中器时的**Monitoring > Statistics > IPSec**类似于**show crypto ipsec sa**和**show crypto isakmp sa** on命令路由器，您能查看IPsec和IKE统计信息。
2. 类似于**show crypto engine connections active命令**在路由器，您能使用在VPN集中器的Administration-Sessions窗口查看参数和统计信息所有活动IPSec LAN-to-LAN连接或通道的。

故障排除

本部分提供的信息可用于对配置进行故障排除。

排除路由器故障

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto engine** - 显示已加密的流量。加密引擎是进行加密和解密的实际机制。加密引擎可以是软件或硬件加速器。
- **debug crypto isakmp** —显示IKE相位1.的互联网安全协会和密钥管理协议(ISAKMP)协商。
- **debug crypto ipsec** - 显示 IKE 第 2 阶段的 IPsec 协商。

参考的IPSec排除故障-了解和使用调试指令欲知更多详细信息和输出示例:。

排除故障VPN集中器

类似于Cisco路由器的debug命令，您能配置事件类型，以查看所有告警。

1. 选择**Configuration > System > Events > Classes > Add**启用登录事件类。这些类为IPsec是可用的：IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE
2. 当添加时，您还能为每个组选择严重级别，警告是根据根据这些安全级别发送的。报警可以由这些方法之一处理：由日志显示在控制台发送对UNIX系统日志服务器发送作为电子邮件发送作为陷阱对简单网络管理协议(SNMP)服务器
3. 选择**Monitoring > Filterable Event Log**监控已启用报警。

相关信息

- 高级加密标准 (AES)
- DES/3DES/AES VPN加密模块

- VPN集中器软件升级
- VPN集中器-版本注释
- 配置IP接口的VPN集中器
- IPSec配置示例
- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPsec 协商/IKE 协议支持页
- 技术支持和文档 - Cisco Systems