

配置 Cisco Secure VPN Client 1.1 for Windows 到 IOS 的连接，以使用本地扩展验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[VPN Client 1.1 安装](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[调试输出示例](#)

[相关信息](#)

简介

本文显示本地扩展认证的(Xauth)配置示例与VPN客户端。此功能提供验证给有思科安全VPN客户端 1.1已安装在他们的PC通过提示用户名和密码的用户的用户。参考[配置Cisco VPN Client 3.x for Windows对IOS使用本地扩展认证](#)关于相同的配置的信息使用Cisco VPN Client 3.x (建议使用)。

先决条件

要求

Xauth可能为[TACACS+和RADIUS](#)也配置与VPN客户端。

Xauth 仅包括身份验证，不包括授权（用户可以在建立连接之后离开）。未实现记帐（用户已离开）。

在您实现Xauth前，配置必须工作，不用Xauth。在本文的示例展示模式配置(模式配置)除Xauth之外，和网络地址转换(NAT)，但是假定是IPSec连通性存在，在Xauth命令被添加前。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- VPN 客户端版本 1.1 (或更高版本)
- Cisco IOS软件版本12.1.2.2.T , 12.1.2.2.P (或以上)
- 运行c3660-jo3s56i-mz.121-2.3.T的本地认证用Cisco 3660测试

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

本文档使用此网络设置。

VPN Client 1.1 安装

Network Security policy:

```
1- Myconn
    My Identity = ip address
        Connection security: Secure
        Remote Party Identity and addressing
            ID Type: IP subnet
            10.21.1.0 (range of inside network)
            Port all Protocol all

        Connect using secure tunnel
            ID Type: IP address
            99.99.99.1
            Pre-shared key = cisco1234

    Authentication (Phase 1)
    Proposal 1
        Authentication method: pre-shared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life: Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

2- Other Connections
    Connection security: Non-secure
    Local Network Interface
```

Name: Any
IP Addr: Any
Port: All

当Xauth启用在路由器，当用户设法连接到一个设备在路由器里面(此处ping -t -.-.-执行)时，一张灰色画面出现：

User Authentication for 3660
Username:
Password:

配置

本地Xauth的路由器配置

```
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-e4-3660
!
!--- Required for Xauth. aaa new-model AAA
authentication login default line !--- Defines the list
for Xauth. AAA authentication login xauth_list local !
username john password 0 doe ! memory-size iomem 30 ip
subnet-zero ! ip audit notify log ip audit po max-events
100 cns event-service server ! !--- Defines IKE policy.
Default encryption is DES. !--- If you want to have 3DES
encryption for IKE and your image is !--- a 3DES image,
put "encryption 3des" under the ISAKMP !--- policy
configuration mode. !--- This must match the parameters
in the "Authentication (Phase 1)" proposal !--- on the
VPN Client. crypto isakmp policy 10 hash md5
authentication pre-share !--- Wildcard pre-shared key
for all the clients. crypto isakmp key cisco1234 address
0.0.0.0 0.0.0.0 !--- Address pool for client-mode
configuration addresses. crypto isakmp client
configuration address-pool local ourpool !--- Define the
IPsec transform set. !--- These parameters must match
Phase 2 proposal parameters !--- configured on the
client. !--- If you have 3DES image and would like to
encrypt your data using 3DES, !--- the line appears as
follows: !--- crypto ipsec transform-set ts esp-3des
esp-md5-hmac. crypto ipsec transform-set mypolicy esp-
des esp-md5-hmac !--- Create a dynamic crypto map that
specifies the transform set to use. crypto dynamic-map
dyna 10 set transform-set mypolicy ! !--- Enable the
Xauth with the specified list. crypto map test client
authentication list xauth_list !--- Enable ModeConfig
initiation and response. crypto map test client
configuration address initiate crypto map test client
configuration address respond !--- Create regular crypto
map based on the dynamic crypto map. crypto map test 5
ipsec-isakmp dynamic dyna ! interface FastEthernet0/0 ip
address 10.21.1.48 255.255.255.0 ip nat inside duplex
auto speed auto ! interface FastEthernet0/1 ip address
99.99.99.1 255.255.255.0 ip Nat outside no ip route-
cache no ip mroute-cache duplex auto speed 10 !--- Apply
the crypto map to the public interface of the router.
crypto map test ! interface Ethernet2/0 no ip address
shutdown ! interface Ethernet2/1 no ip address shutdown
```

```
! !--- Define the pool of addresses for ModeConfig (see
reference !--- earlier in this output). ip local pool
ourpool 10.2.1.1 10.2.1.254 ip Nat pool outsidepool
99.99.99.50 99.99.99.60 netmask 255.255.255.0 ip Nat
inside source route-map nonat pool outsidepool ip
classless ip route 0.0.0.0 0.0.0.0 10.21.1.1 no ip http
server ! access-list 101 deny ip 10.21.1.0 0.0.0.255
10.2.1.0 0.0.0.255 access-list 101 permit ip 10.21.1.0
0.0.0.255 any route-map nonat permit 10 match ip address
101 ! line con 0 transport input none line aux 0 line
vty 0 4 password ww ! end
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

[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 aaa authentication** - 显示 AAA/TACACS+ 身份验证的信息。
- **debug crypto isakmp** — 显示关于 IKE 事件的消息。
- **debug crypto ipsec** — 显示 IPsec 事件。
- **debug crypto key-exchange** - 显示数字签字标准 (DSS) 公钥交换消息。
- **clear crypto isakmp** - 指定要清除的连接。
- **clear crypto sa** — 删除IPsec安全关联。

调试输出示例

```
goss-e4-3660#show debug General OS: AAA Authentication debugging is on Cryptographic Subsystem:
Crypto ISAKMP debugging is on Crypto Engine debugging is on Crypto IPSEC debugging is on
goss-e4-3660#term mon goss-e4-3660# 01:37:58: ISAKMP (0:0): received packet from 99.99.99.5 (N) NEW
SA 01:37:58: ISAKMP: local port 500, remote port 500 01:37:58: ISAKMP (0:1): Setting client
config settings 627D1E3C 01:37:58: ISAKMP (0:1): (Re)Setting client xauth list xauth_list and
state 01:37:58: ISAKMP: Created a peer node for 99.99.99.5 01:37:58: ISAKMP: Locking struct
627D1E3C from crypto_ikmp_config_initialize_sa 01:37:58: ISAKMP (0:1): processing SA payload.
message ID = 0 !--- Pre-shared key matched. 01:37:58: ISAKMP (0:1): found peer pre-shared key
matching 99.99.99.5 01:37:58: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10
policy 01:37:58: ISAKMP: encryption DES-CBC 01:37:58: ISAKMP: hash MD5 01:37:58: ISAKMP: default
group 1 01:37:58: ISAKMP: auth pre-share !--- ISAKMP policy proposed by VPN Client matched the
configured ISAKMP policy. 01:37:58: ISAKMP (0:1): atts are acceptable. Next payload is 0
01:37:58: CryptoEngine0: generate alg parameter 01:37:58: CRYPTO_ENGINE: Dh phase 1 status: 0
01:37:58: CRYPTO_ENGINE: DH phase 1 status: 0 01:37:58: ISAKMP (0:1): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR 01:37:58: ISAKMP (0:1): sending packet to 99.99.99.5
(R) MM_SA_SETUP 01:37:59: ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_SA_SETUP
01:37:59: ISAKMP (0:1): processing KE payload. Message ID = 0 01:37:59: CryptoEngine0: generate
alg parameter 01:37:59: ISAKMP (0:1): processing NONCE payload. Message ID = 0 01:37:59: ISAKMP
```

(0:1): found peer pre-shared key matching 99.99.99.5 01:37:59: CryptoEngine0: create ISAKMP SKEYID for conn id 1 01:37:59: ISAKMP (0:1): SKEYID state generated 01:37:59: ISAKMP (0:1): processing vendor id payload 01:37:59: ISAKMP (0:1): processing vendor id payload 01:37:59: ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_KEY_EXCH 01:37:59: ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_KEY_EXCH 01:37:59: ISAKMP (0:1): processing ID payload. Message ID = 0 01:37:59: ISAKMP (0:1): processing HASH payload. Message ID = 0 01:37:59: CryptoEngine0: generate hmac context for conn id 1 01:37:59: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1 spi 0, message ID = 0 01:37:59: ISAKMP (0:1): SA has been authenticated with 99.99.99.5 01:37:59: ISAKMP (1): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 01:37:59: ISAKMP (1): Total payload length: 12 01:37:59: CryptoEngine0: generate hmac context for conn id 1 01:37:59: CryptoEngine0: clear DH number for conn id 1 **!--- Starting Xauth.** 01:37:59: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH 01:38:00: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH 01:38:00: ISAKMP (0:1): (Re)Setting client xauth list xauth_list and state 01:38:00: ISAKMP (0:1): Need XAUTH 01:38:00: AAA: parse name=ISAKMP idb type=-1 tty=-1 01:38:00: AAA/MEMORY: create_user (0x627D27D0) user='' ruser='' port='ISAKMP' rem_addr='99.99.99.5' authen_type=ASCII service=LOGIN priv=0 01:38:00: AAA/AUTHEN/START (324819201): port='ISAKMP' list='xauth_list' action=LOGIN service=LOGIN 01:38:00: AAA/AUTHEN/START (324819201): found list xauth_list 01:38:00: AAA/AUTHEN/START (324819201): Method=LOCAL 01:38:00: AAA/AUTHEN (324819201): status = GETUSER 01:38:00: ISAKMP: got callback 1 01:38:00: ISAKMP/xauth: request attribute XAUTH_TYPE 01:38:00: ISAKMP/xauth: request attribute XAUTH_MESSAGE 01:38:00: ISAKMP/xauth: request attribute XAUTH_USER_NAME 01:38:00: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD 01:38:00: CryptoEngine0: generate hmac context for conn id 1 01:38:00: ISAKMP (0:1): initiating peer config to 99.99.99.5. ID = 944484565 01:38:00: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH 01:38:02: IPSEC(decapsulate): error in decapsulation crypto_ipsec_sa_exists **!--- The user has delayed the input of the username/password.** 01:38:05: ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH 944484565 ... 01:38:05: ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2 01:38:05: ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2 01:38:05: ISAKMP (0:1): retransmitting phase 2 944484565 CONF_XAUTH 01:38:05: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH 01:38:08: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH 01:38:08: ISAKMP (0:1): processing transaction payload from 99.99.99.5. Message ID = 944484565 01:38:08: CryptoEngine0: generate hmac context for conn id 1 01:38:08: ISAKMP: Config payload REPLY 01:38:08: ISAKMP/xauth: reply attribute XAUTH_TYPE 01:38:08: ISAKMP/xauth: reply attribute XAUTH_USER_NAME 01:38:08: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD 01:38:08: AAA/AUTHEN/CONT (324819201): continue_login (user='(undef)') 01:38:08: AAA/AUTHEN (324819201): status = GETUSER 01:38:08: AAA/AUTHEN/CONT (324819201): Method=LOCAL 01:38:08: AAA/AUTHEN (324819201): status = GETPASS 01:38:08: AAA/AUTHEN/CONT (324819201): continue_login (user='john') 01:38:08: AAA/AUTHEN (324819201): status = GETPASS 01:38:08: AAA/AUTHEN/CONT (324819201): Method=LOCAL 01:38:08: AAA/AUTHEN (324819201): status = PASS 01:38:08: ISAKMP: got callback 1 01:38:08: CryptoEngine0: generate hmac context for conn id 1 01:38:08: ISAKMP (0:1): initiating peer config to 99.99.99.5. ID = 944484565 01:38:08: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH 01:38:08: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH 01:38:08: ISAKMP (0:1): processing transaction payload from 99.99.99.5. Message ID = 944484565 01:38:08: CryptoEngine0: generate hmac context for conn id 1 01:38:08: ISAKMP: Config payload ACK **!--- Xauth finished.** 01:38:08: ISAKMP (0:1): deleting node 944484565 error FALSE reason "done with transaction" 01:38:08: ISAKMP (0:1): allocating address 10.2.1.2 01:38:08: CryptoEngine0: generate hmac context for conn id 1 01:38:08: ISAKMP (0:1): initiating peer config to 99.99.99.5. ID = -2139076758 01:38:08: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_ADDR 01:38:08: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_ADDR 01:38:08: ISAKMP (0:1): processing transaction payload from 99.99.99.5. Message ID = -2139076758 01:38:08: CryptoEngine0: generate hmac context for conn id 1 01:38:08: ISAKMP: Config payload ACK 01:38:08: ISAKMP (0:1): peer accepted the address! 01:38:08: ISAKMP (0:1): adding static route for 10.2.1.2 01:38:08: ISAKMP (0:1): installing route 10.2.1.2 255.255.255.255 99.99.99.5 01:38:08: ISAKMP (0:1): deleting node -2139076758 error FALSE reason "done with transaction" 01:38:08: ISAKMP (0:1): Delaying response to QM request. 01:38:09: ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE 01:38:09: ISAKMP (0:1): (Re)Setting client xauth list xauth_list and state 01:38:09: CryptoEngine0: generate hmac context for conn id 1 01:38:09: ISAKMP (0:1): processing HASH payload. Message ID = -1138778119 01:38:09: ISAKMP (0:1): processing SA payload. Message ID = -1138778119 01:38:09: ISAKMP (0:1): Checking IPsec proposal 1 01:38:09: ISAKMP: transform 1, ESP_DES 01:38:09: ISAKMP: attributes in transform: 01:38:09: ISAKMP: authenticator is HMAC-MD5 01:38:09: ISAKMP: encaps is 1 01:38:09: validate proposal 0 **!--- Proposed Phase 2 transform set matched configured IPsec transform set.** 01:38:09: ISAKMP (0:1): atts are acceptable. 01:38:09: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest=99.99.99.1, src=99.99.99.5, dest_proxy=10.21.1.0/255.255.255.0/0/0 (type=4), src_proxy=

```
10.2.1.2/255.255.255.255/0/0 (type=1), protocol= ESP, transform= ESP-Des esp-md5-hmac , lifedur=
0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 01:38:09: validate proposal request
0 01:38:09: ISAKMP (0:1): processing NONCE payload. Message ID = -1138778119 01:38:09: ISAKMP
(0:1): processing ID payload. Message ID = -1138778119 01:38:09: ISAKMP (1): ID_IPV4_ADDR src
10.2.1.2 prot 0 port 0 01:38:09: ISAKMP (0:1): processing ID payload. Message ID = -1138778119
01:38:09: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 10.21.1.0/255.255.255.0 prot 0 port 0 01:38:09:
ISAKMP (0:1): asking for 1 spis from ipsec 01:38:09: IPSEC(key_engine): got a queue event...
01:38:09: IPSEC(spi_response): getting spi 3339398037 for SA from 99.99.99.5 to 99.99.99.1 for
prot 3 01:38:09: ISAKMP: received ke message (2/1) 01:38:10: CryptoEngine0: generate hmac
context for conn id 1 01:38:10: ISAKMP (0:1): sending packet to 99.99.99.5 (R) QM_IDLE 01:38:10:
ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE 01:38:10: CryptoEngine0: generate hmac
context for conn id 1 01:38:10: ipsec allocate flow 0 01:38:10: ipsec allocate flow 0 01:38:10:
ISAKMP (0:1): Creating IPsec SAs 01:38:10: inbound SA from 99.99.99.5 to 99.99.99.1 (proxy
10.2.1.2 to 10.21.1.0) 01:38:10: has spi 0xC70B2B95 and conn_id 2000 and flags 4 01:38:10:
outbound SA from 99.99.99.1 to 99.99.99.5 (proxy 10.21.1.0 to 10.2.1.2) 01:38:10: has spi -
1679939467 and conn_id 2001 and flags 4 01:38:10: ISAKMP (0:1): deleting node -1769610309 error
FALSE reason "saved qm no longer needed" 01:38:10: ISAKMP (0:1): deleting node -1138778119 error
FALSE reason "quick mode done (await())" 01:38:10: IPSEC(key_engine): got a queue event... !---
IPsec SAs created. 01:38:10: IPSEC(initialize_sas): , (key Eng. msg.) dest= 99.99.99.1, src=
99.99.99.5, dest_proxy= 10.21.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.2.1.2/0.0.0.0/0/0
(type=1), protocol= ESP, transform= ESP-Des esp-md5-hmac , lifedur= 0s and 0kb, spi=
0xC70B2B95(3339398037), conn_id= 2000, keysize= 0, flags= 0x4 01:38:10: IPSEC(initialize_sas): ,
(key Eng. msg.) src= 99.99.99.1, dest= 99.99.99.5, src_proxy= 10.21.1.0/255.255.255.0/0/0
(type=4), dest_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1), protocol= ESP, transform= ESP-Des esp-md5-
hmac , lifedur= 0s and 0kb, spi= 0x9BDE2875(2615027829), conn_id= 2001, keysize= 0, flags= 0x4
01:38:10: IPSEC(create_sa): sa created, (sa) sa_dest= 99.99.99.1, sa_prot= 50, sa_spi=
0xC70B2B95(3339398037), sa_trans= ESP-Des esp-md5-hmac , sa_conn_id= 2000 01:38:10:
IPSEC(create_sa): sa created, (sa) sa_dest= 99.99.99.5, sa_prot= 50, sa_spi=
0x9BDE2875(2615027829), sa_trans= ESP-Des esp-md5-hmac , sa_conn_id= 2001 01:38:10: ISAKMP:
received ke message (4/1) 01:38:10: ISAKMP: Locking struct 627D1E3C for IPSEC
```

相关信息

- [EOS和EOL思科安全VPN客户端的](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)