

Configuring Cisco Secure VPN Client 1.1 for Windows to IOS Using Local Extended Authentication (Configurando o Cisco Secure VPN Client 1.1 para Windows para IOS utilizando autenticação estendida local)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração do VPN Client 1.1](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Exemplo de debug](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento mostra configurações de amostra para a autenticação estendida local (Xauth) com o cliente VPN. Esta característica fornece a autenticação a um usuário que tenha o Cisco Secure VPN Client 1.1 instalado em seu PC alertando o usuário para um username e uma senha. Refira [configurar o Cisco VPN Client 3.x para Windows aos IO usando a autenticação estendida local](#) para obter informações sobre da mesma configuração usando o Cisco VPN Client 3.x (recomendado).

[Pré-requisitos](#)

[Requisitos](#)

O Xauth pode igualmente ser configurado para o [TACACS+ e o RADIUS](#) com cliente VPN.

O Xauth inclui a *autenticação* somente, não *autorização* (onde os usuários podem ir uma vez a

conexão são estabelecidos). *Explicar* (onde os usuários foram) não é executado.

A configuração deve trabalhar sem Xauth antes que você execute o Xauth. O exemplo neste documento demonstra a configuração de modo (config de modo) e o Network Address Translation (NAT) além do que o Xauth, mas a suposição é que a conectividade IPSec esta presente antes que os comandos xauth estejam adicionados.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 1.1 do cliente VPN (ou mais tarde)
- Software Release 12.1.2.2.T de Cisco IOS®, 12.1.2.2.P (ou mais tarde)
- A autenticação local foi testada com um Cisco 3660 que executa c3660-jo3s56i-mz.121-2.3.T

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.

Configuração do VPN Client 1.1

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
```

Com o Xauth permitido no roteador, quando o usuário tenta conectar a um dispositivo dentro do roteador (um ping - t #.#.#.# esteve executado aqui), uma tela cinzenta aparece:

```
User Authentication for 3660
Username:
Password:
```

Configurações

Configuração de roteador para o xauth local

```
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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debug aaa authentication** — Exibe informações sobre autenticação AAA/TACACS+.
- **debug crypto isakmp** - Exibe mensagens sobre eventos IKE.
- **debug crypto ipsec** — Exibe eventos de IPSec.
- **debug crypto key-exchange** — Mensagens de intercâmbio da chave pública do Digital Signature Standard (DSS) das mostras.
- **cancela o isakmp cripto** — Especifica que conexão a cancelar.

- **cancela o sa cripto** — Associações de segurança IPsec das supressões.

Exemplo de debug

```
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

[Informações Relacionadas](#)

- [EOS e EOL para o Cisco Secure VPN Client](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)