로컬 확장 인증을 사용하여 Windows용 Cisco Secure VPN Client 1.1을 IOS로 구성

목차

소개

이 문서에서는 VPN 클라이언트를 사용하는 로컬 Extended Authentication(Xauth)에 대한 샘플 컨피그레이션을 보여줍니다. 이 기능은 Cisco Secure VPN Client 1.1이 PC에 설치된 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하여 인증을 제공합니다. Cisco VPN Client 3.x를 사용하는 동일한 컨피그레이션에 대한 자세한 내용은 Windows용 Cisco VPN Client 3.x를 IOS로 구성 로컬 확장 인증 사용(권장)을 참조하십시오.

사전 요구 사항

요구 사항

VPN 클라이언트를 사용하여 TACACS+ 및 RADIUS에 대해 Xauth를 구성할 수도 있습니다.

Xauth에는 *인증*만 포함되며 *권한*은 부여되지 않습니다(연결이 설정되면 사용자가 이동할 수 있음). *계정*(사용자가 이동한 경우)은 구현되지 않습니다.

Xauth를 구현하려면 먼저 Xauth 없이 컨피그레이션이 작동해야 합니다. 이 문서의 예에서는 Xauth 외에 Mode Configuration(Mode Config) 및 NAT(Network Address Translation)를 보여 주지만, Xauth 명령을 추가하기 전에 IPsec 연결이 있다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN 클라이언트 버전 1.1 이상
- Cisco IOS® 소프트웨어 릴리스 12.1.2.2.T, 12.1.2.2.P(이상)
- 로컬 인증은 c3660-jo3s56i-mz.121-2.3.T를 실행하는 Cisco 3660에서 테스트되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

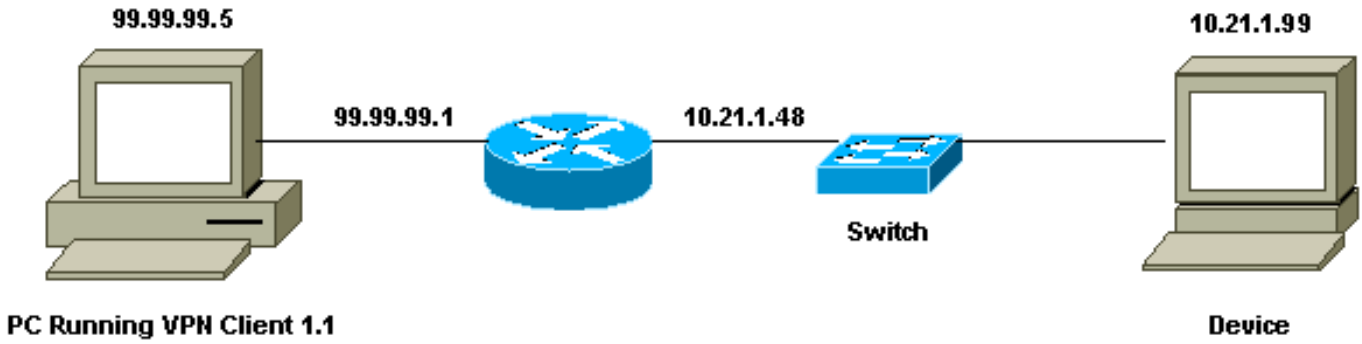
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



VPN 클라이언트 1.1 설정

```
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
```

라우터에서 Xauth가 활성화된 상태에서 사용자가 라우터 내의 디바이스에 연결을 시도할 때(**ping -t #.#.#**이 수행됨) 회색 화면이 나타납니다.

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

구성

로컬 Xauth에 대한 라우터 컨피그레이션

```
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
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug aaa authentication**—AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.
- **debug crypto ipsec** - IPsec 이벤트를 표시합니다.
- **debug crypto key-exchange** - DSS(Digital Signature Standard) 공개 키 교환 메시지를 표시합니다.
- **clear crypto isakmp** - 지울 연결을 지정합니다.
- **clear crypto sa** - IPsec 보안 연결을 삭제합니다.

디버그 출력 샘플

```
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
```

관련 정보

- Cisco Secure VPN Client용 EOS 및 EOL
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems