Cliente VPN sobre LAN Wireless com Exemplo de Configuração de WLC

Contents

Introduction

Este documento apresenta o conceito de Rede Virtual Privada (VPN - Virtual Private Network) em um ambiente sem fio. O documento explica as configurações envolvidas na implantação de um túnel VPN entre um cliente sem fio e um servidor VPN através de um Wireless LAN Controller (WLC).

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento das WLCs e como configurar os parâmetros básicos da WLC
- Conhecimento dos conceitos de WPA (Wi-Fi Protected Access)
- Conhecimento básico da VPN e seus tipos
- Conhecimento de IPsec
- Conhecimento básico dos algoritmos de criptografia, autenticação e hash disponíveis

Componentes Utilizados

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

- Cisco 2006 WLC que executa a versão 4.0.179.8
- Access Point Lightweight (LAP) Cisco 1000 Series
- Cisco 3640 que executa o Cisco IOS® Software Release 12.4(8)
- Cisco VPN Client versão 4.8

Observação: este documento usa um roteador 3640 como um servidor VPN. Para suportar recursos de segurança mais avançados, você também pode usar um servidor VPN dedicado.

Observação: para que um roteador atue como um servidor VPN, ele precisa executar um conjunto de recursos que suporte IPsec básico.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Uma VPN é uma rede de dados privada que é usada para transmitir dados com segurança em uma rede privada através da infraestrutura de telecomunicações públicas, como a Internet. Essa VPN mantém a privacidade dos dados por meio do uso de um protocolo de tunelamento e procedimentos de segurança.

VPN de acesso remoto

Uma configuração de VPN de acesso remoto é usada para permitir que clientes de software VPN, como usuários móveis, acessem com segurança recursos de rede centralizados que residem atrás de um servidor VPN. Nas terminologias da Cisco, esses servidores e clientes VPN também são chamados de servidor Cisco Easy VPN e dispositivo Cisco Easy VPN Remote.

Um dispositivo Cisco Easy VPN Remote pode ser Cisco IOS Routers, Cisco PIX Security Appliances, Cisco VPN 3002 Hardware Clients e Cisco VPN Client. Eles são usados para receber políticas de segurança em uma conexão de túnel VPN de um Cisco Easy VPN Server. Isso minimiza os requisitos de configuração no local remoto. O Cisco VPN Client é um cliente de software que pode ser instalado em PCs, laptops e assim por diante.

Um Cisco Easy VPN Server pode ser Cisco IOS Routers, Cisco PIX Security Appliances e Cisco VPN 3000 Concentrators.

Este documento usa o software Cisco VPN Client executado em um laptop como o VPN Client e o Cisco 3640 IOS Router como o servidor VPN. O documento usa o padrão IPsec para estabelecer um túnel VPN entre um cliente e um servidor.

IPsec

O IPsec é uma estrutura de padrões abertos desenvolvida pela Internet Engineering Task Force (IETF). O IPsec fornece segurança para a transmissão de informações confidenciais por redes não protegidas, como a Internet.

O IPsec fornece criptografia de dados de rede no nível de pacote IP, que oferece uma solução de segurança robusta baseada em padrões. A principal tarefa do IPsec é permitir a troca de informações privadas por uma conexão insegura. O IPsec usa criptografia para proteger informações contra interceptação ou escuta. No entanto, para usar a criptografia com eficiência, ambas as partes devem compartilhar um segredo que é usado tanto para a criptografia quanto para a descriptografia das informações.

O IPsec opera em duas fases para permitir a troca confidencial de um segredo compartilhado:

- Fase 1—Trata a negociação dos parâmetros de segurança necessários para estabelecer um canal seguro entre dois pares IPsec. A fase 1 é geralmente implementada através do protocolo IKE (Internet Key Exchange, Intercâmbio de chave de Internet). Se o peer IPsec remoto não puder executar IKE, você poderá usar a configuração manual com chaves pré-compartilhadas para concluir a Fase 1.
- Fase 2—Usa o túnel seguro estabelecido na Fase 1 para trocar os parâmetros de segurança necessários para realmente transmitir dados do usuário. Os túneis seguros usados em ambas as fases do IPsec são baseados em associações de segurança (SAs) usadas em cada ponto final do IPsec. As SAs descrevem os parâmetros de segurança, como o tipo de autenticação e criptografia que ambos os terminais concordam em usar.

Os parâmetros de segurança trocados na Fase 2 são usados para criar um túnel IPsec que, por sua vez, é usado para transferência de dados entre o VPN Client e o servidor.

Consulte Configuração de IPsec para obter mais informações sobre IPsec e sua configuração.

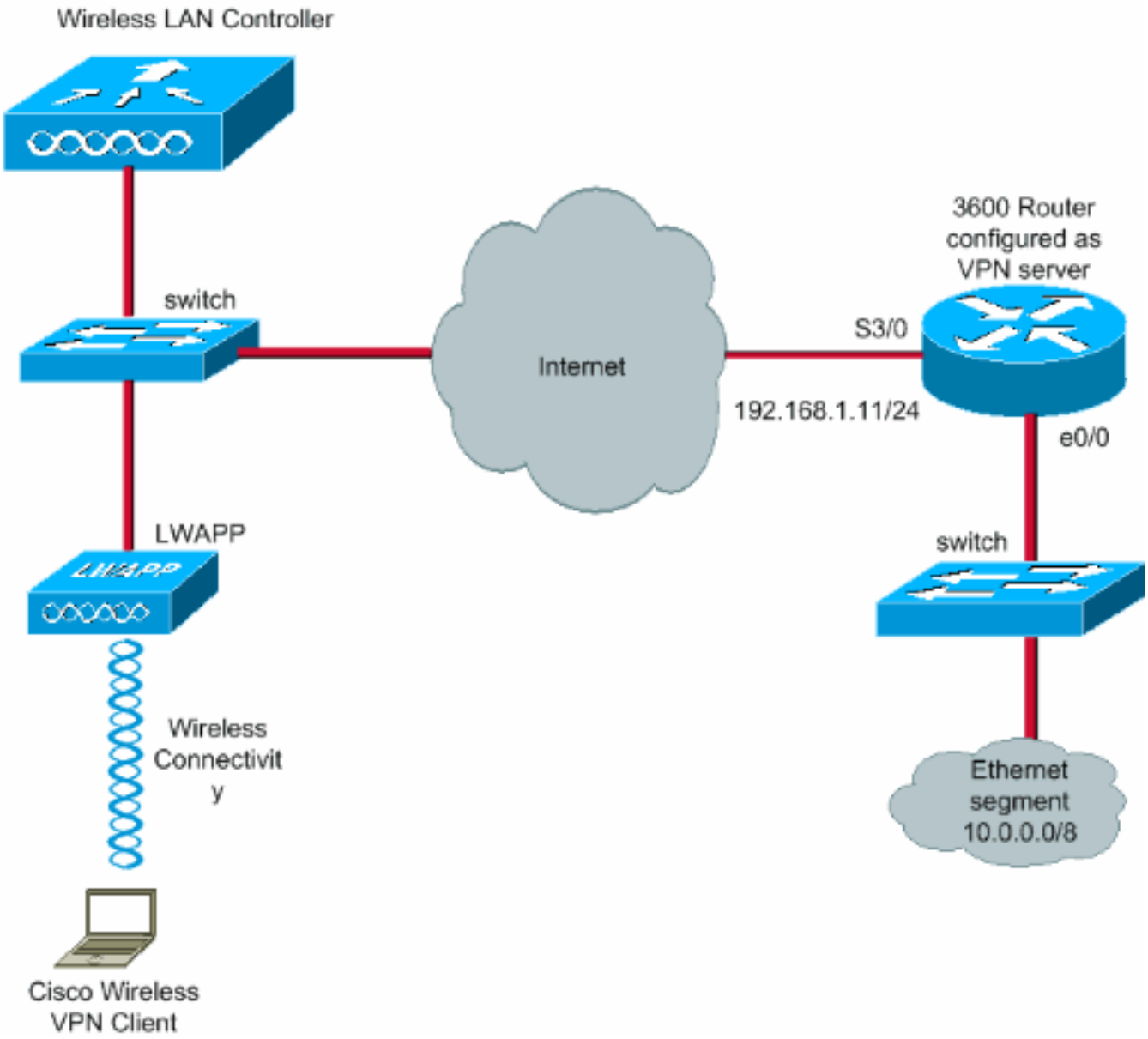
Quando um túnel VPN é estabelecido entre o VPN Client e o servidor, *as políticas de segurança definidas no servidor VPN são enviadas ao cliente*. Isso minimiza os requisitos de configuração no lado do cliente.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza as seguintes configurações:

- Endereço IP da interface de gerenciamento da WLC—172.16.1.10/16
- Endereço IP da interface do gerenciador de AP da WLC—172.16.1.11/16
- Gateway padrão—172.16.1.20/16**Observação:** em uma rede ativa, esse gateway padrão deve apontar para a interface de entrada do roteador imediato que conecta a WLC ao restante da rede e/ou à Internet.
- Endereço IP do servidor VPN s3/0—192.168.1.11/24**Observação:** esse endereço IP deve apontar para a interface que encerra o túnel VPN no lado do servidor VPN. Neste exemplo, s3/0 é a interface que encerra o túnel VPN no servidor VPN.
- O segmento de LAN no servidor VPN usa o intervalo de endereços IP de 10.0.0.0/8.



Configurar

Em uma arquitetura centralizada de WLAN, para permitir que um cliente VPN sem fio, como um laptop, estabeleça um túnel VPN com um servidor VPN, é necessário que o cliente seja associado a um Lightweight Access Point (LAP) que, por sua vez, precisa ser registrado com uma WLC. Este documento tem o LAP como já registrado na WLC usando o processo de descoberta de broadcast de sub-rede local explicado em Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

A próxima etapa é configurar o WLC para VPN.

Terminação e passagem de VPN

Com as WLCs Cisco 4000 Series anteriores à versão 4, um recurso chamado terminação de VPN IPsec (suporte de IPsec) é suportado. Esse recurso permite que esses controladores terminem sessões do VPN Client diretamente no controlador. Em resumo, esse recurso permite que o próprio controlador atue como um servidor VPN. Mas isso exige que um módulo de hardware de terminação VPN separado seja instalado no controlador.

Este suporte de VPN IPsec não está disponível em:

- WLC Cisco 2000 Series
- Qualquer WLC que execute a versão 4.0 ou posterior

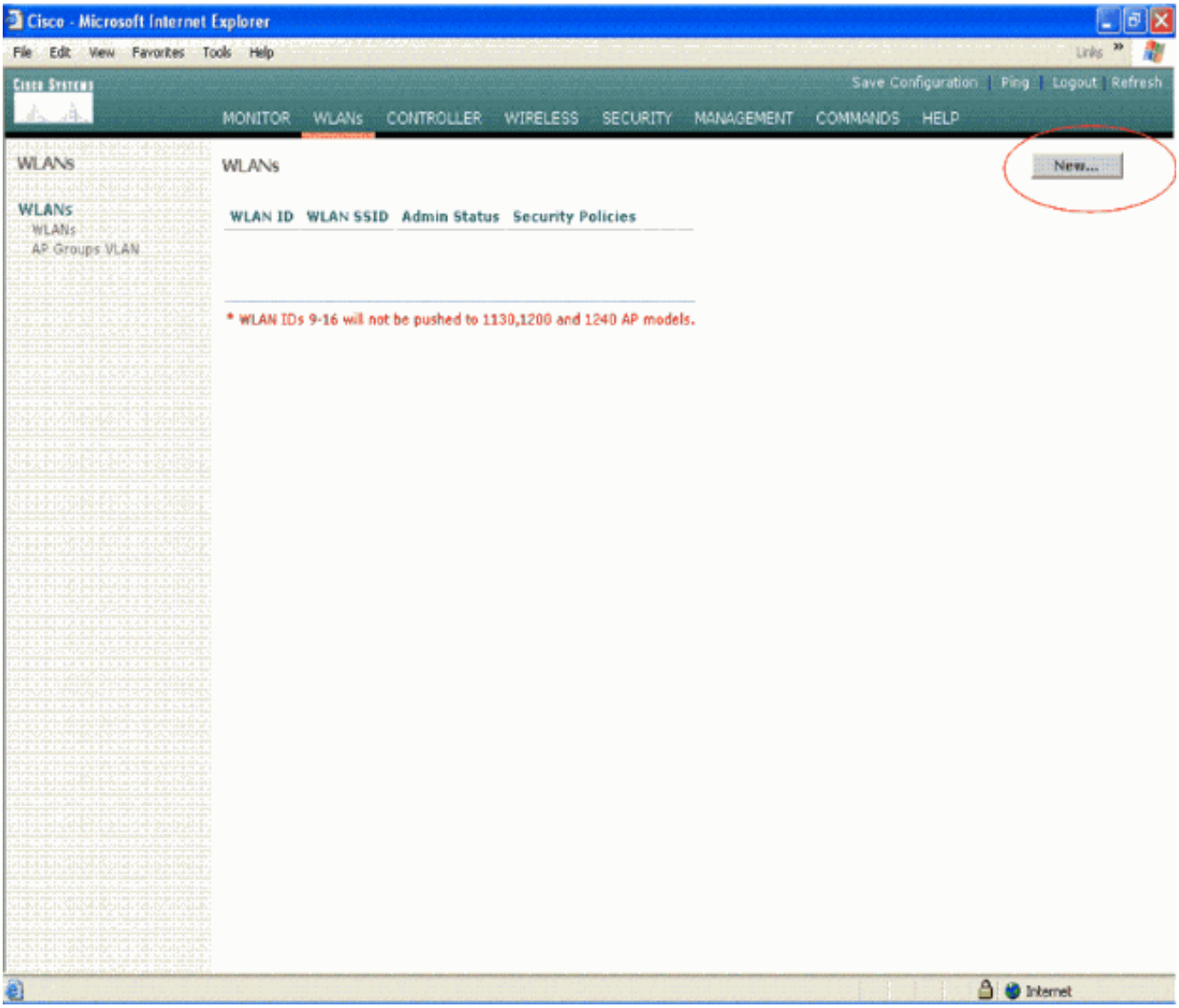
Portanto, o único recurso VPN suportado em versões posteriores à 4.0 é o VPN Pass-through. Esse recurso também é suportado no Cisco 2000 Series WLC.

O VPN Pass-through é um recurso que permite que um cliente estabeleça um túnel somente com um servidor VPN específico. Portanto, se você precisar acessar com segurança o servidor VPN configurado, bem como outro servidor VPN ou a Internet, isso não é possível com o VPN Pass-through ativado no controlador. Sob esses requisitos, você precisa desativar o VPN Pass-through. No entanto, a WLC pode ser configurada para atuar como passagem para acessar vários gateways VPN quando uma ACL apropriada é criada e aplicada à WLAN correspondente. Assim, nesses cenários em que você deseja acessar vários gateways VPN para redundância, desative a passagem de VPN e crie uma ACL que permita o acesso aos gateways VPN e aplique a ACL à WLAN.

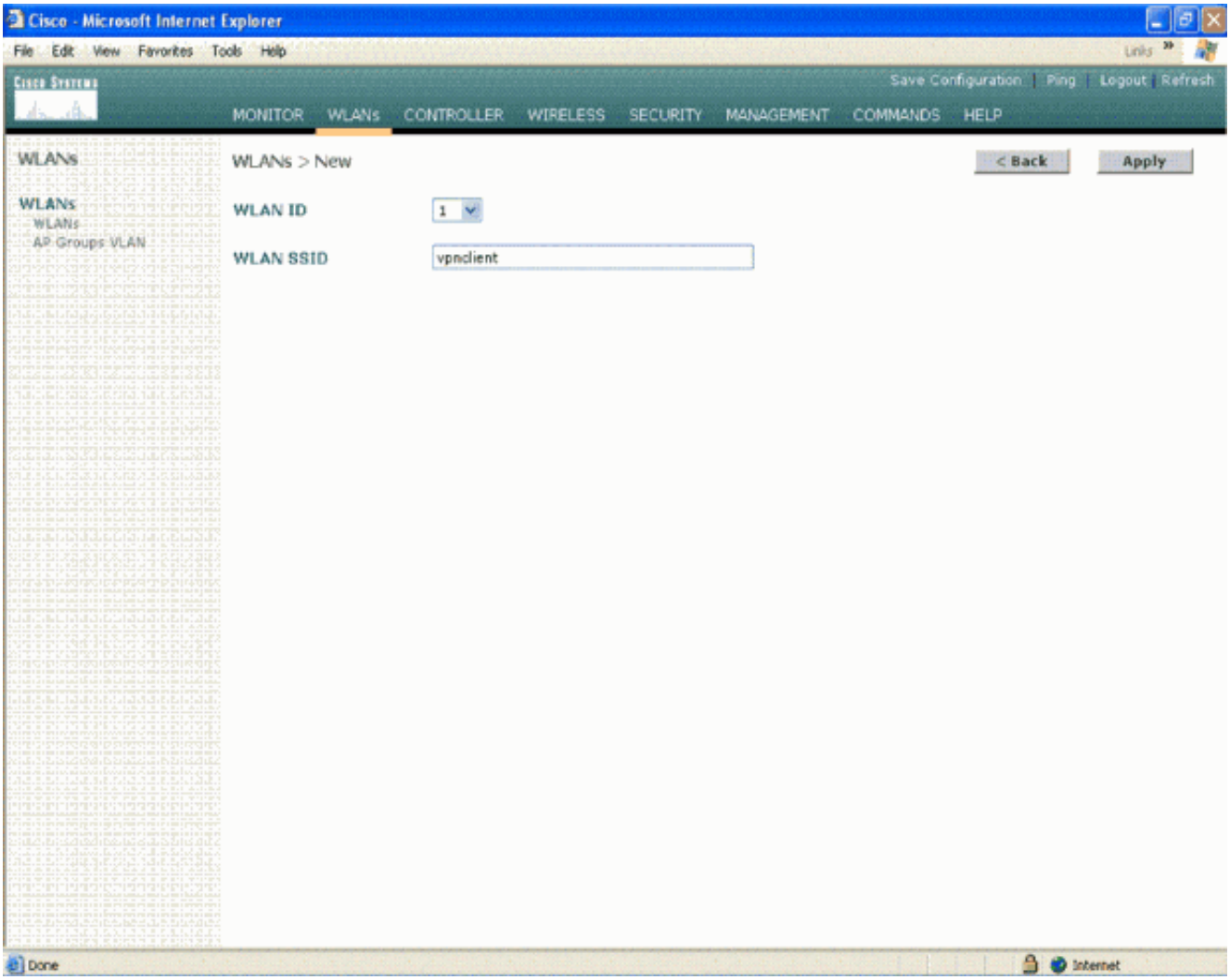
Configurar o WLC para passagem de VPN

Conclua estes passos para configurar o VPN Pass-through.

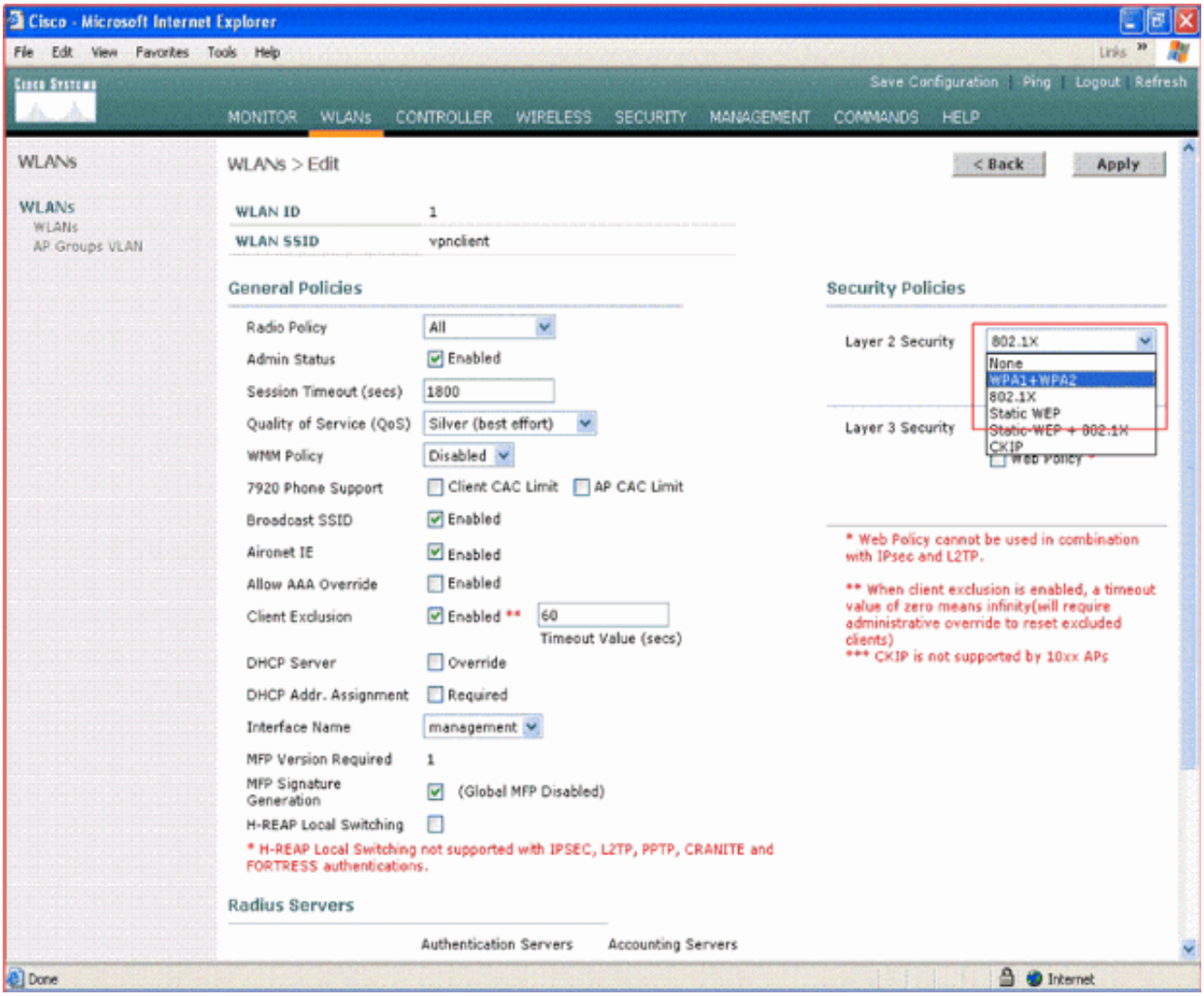
1. Na GUI da WLC, clique em **WLAN** para ir para a página WLANs.
2. Clique em **New** para criar uma nova WLAN.



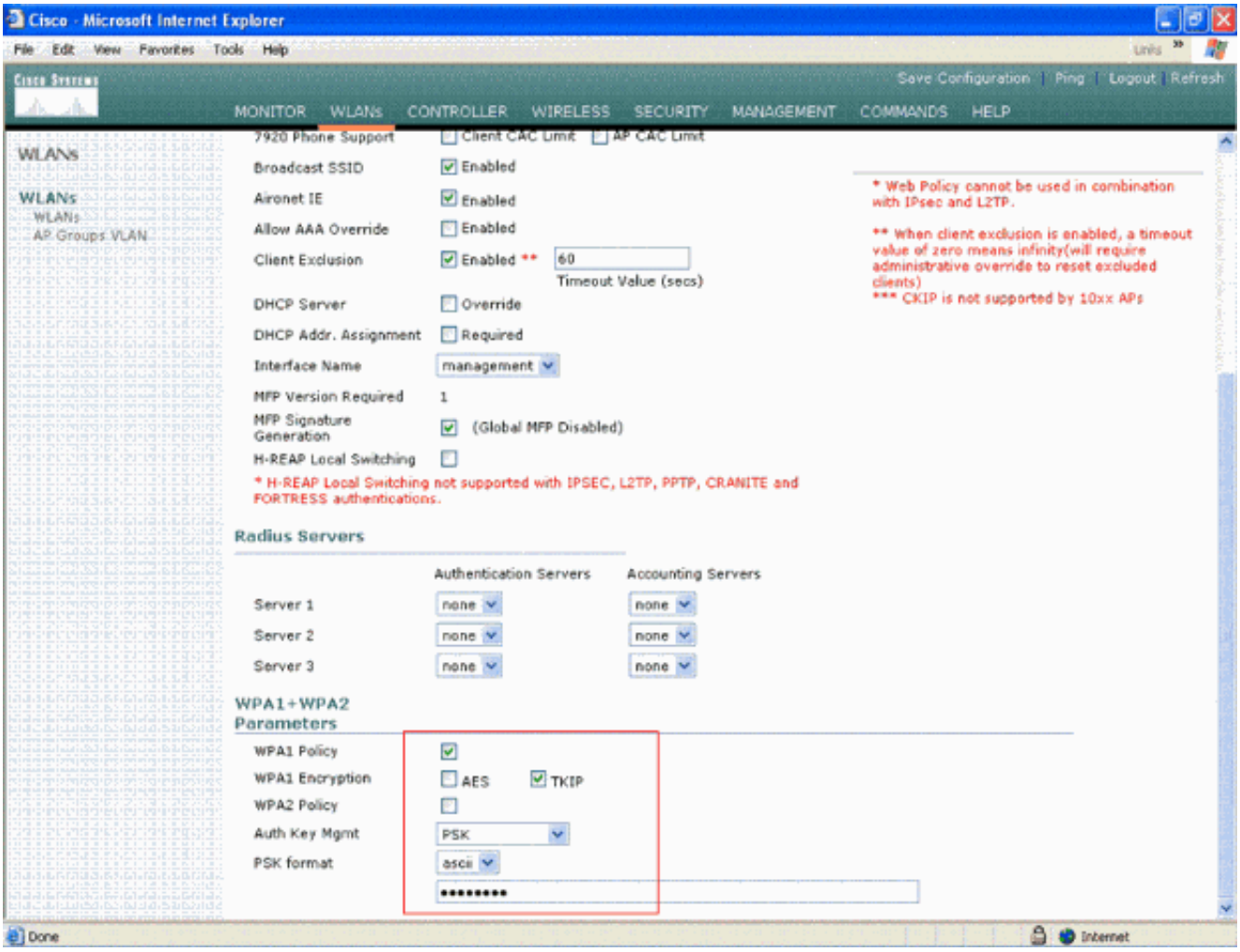
3. O SSID da WLAN é nomeado como **vpnclient** neste exemplo. Clique em Apply.



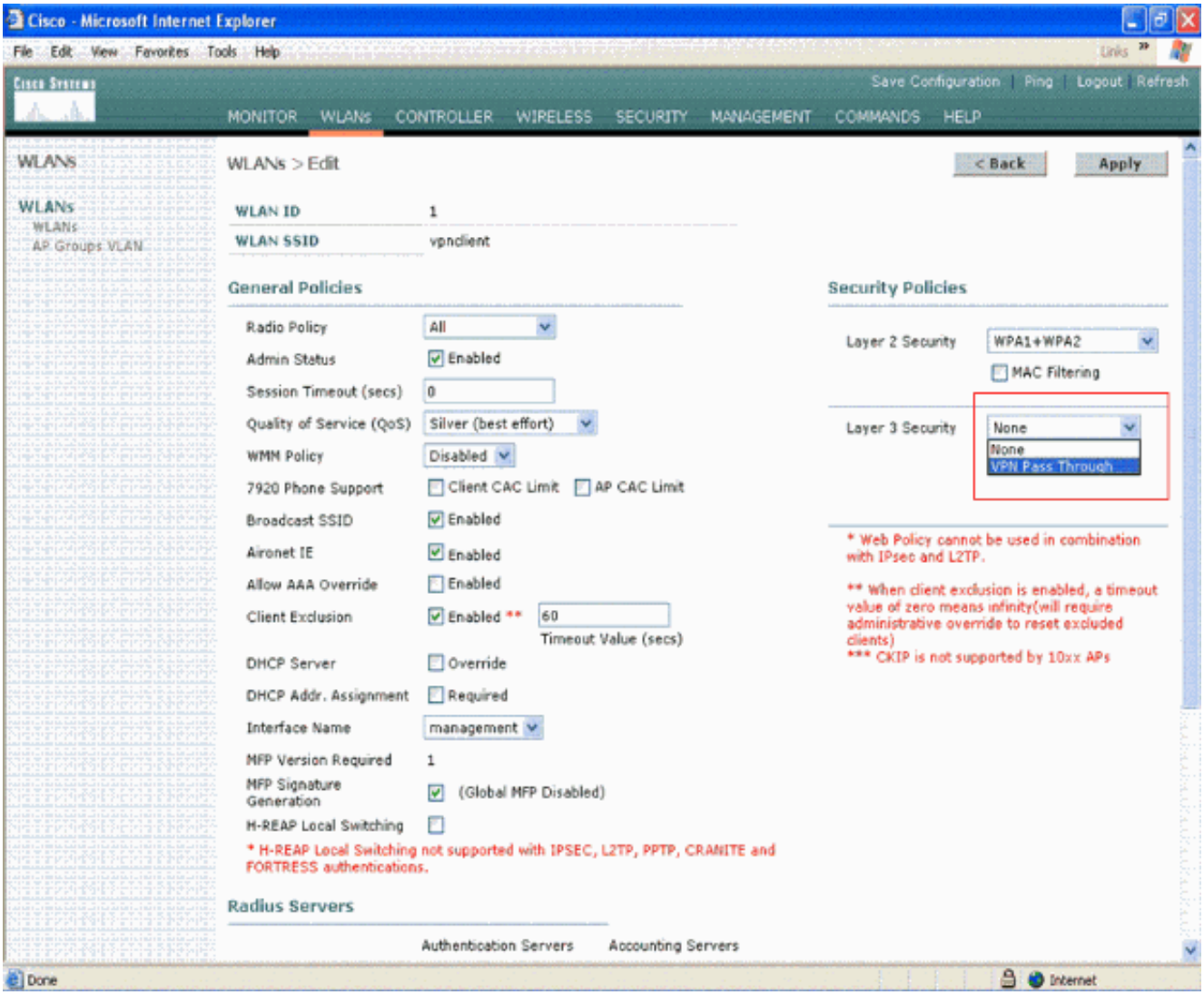
4. Configure o SSID do vpnclient com segurança de Camada 2. *Isso é opcional*.Este exemplo usa **WPA1+WPA2** como o tipo de segurança.



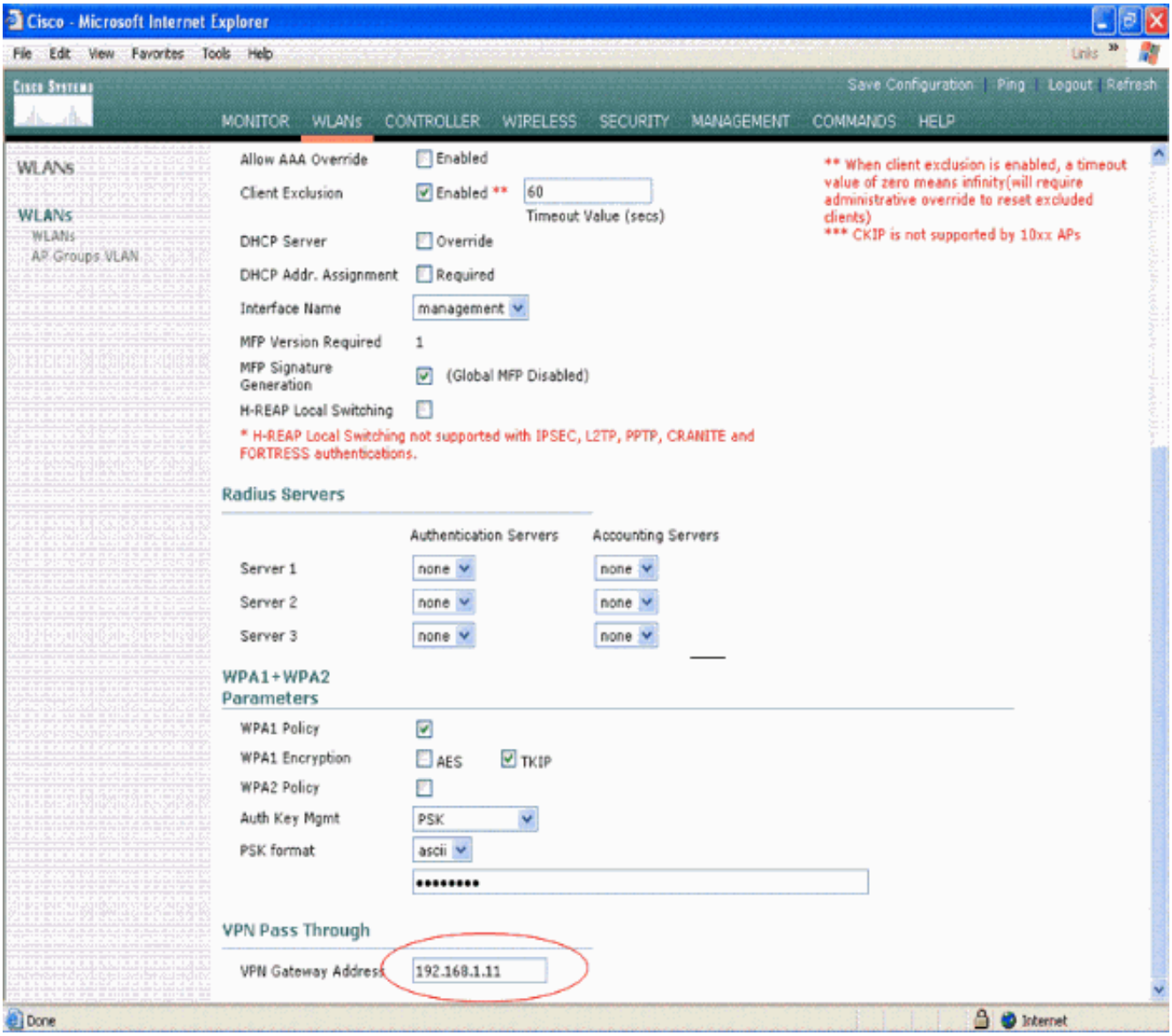
5. Configure a política WPA e o tipo de gerenciamento de chave de autenticação a serem usados.Este exemplo usa a **chave pré-compartilhada (PSK)** para o gerenciamento da chave de autenticação. Depois que PSK for selecionado, selecione **ASCII** como o formato PSK e digite o valor PSK. Esse valor deve ser o mesmo na configuração SSID do cliente sem fio para que os clientes que pertencem a esse SSID se associem a essa WLAN.



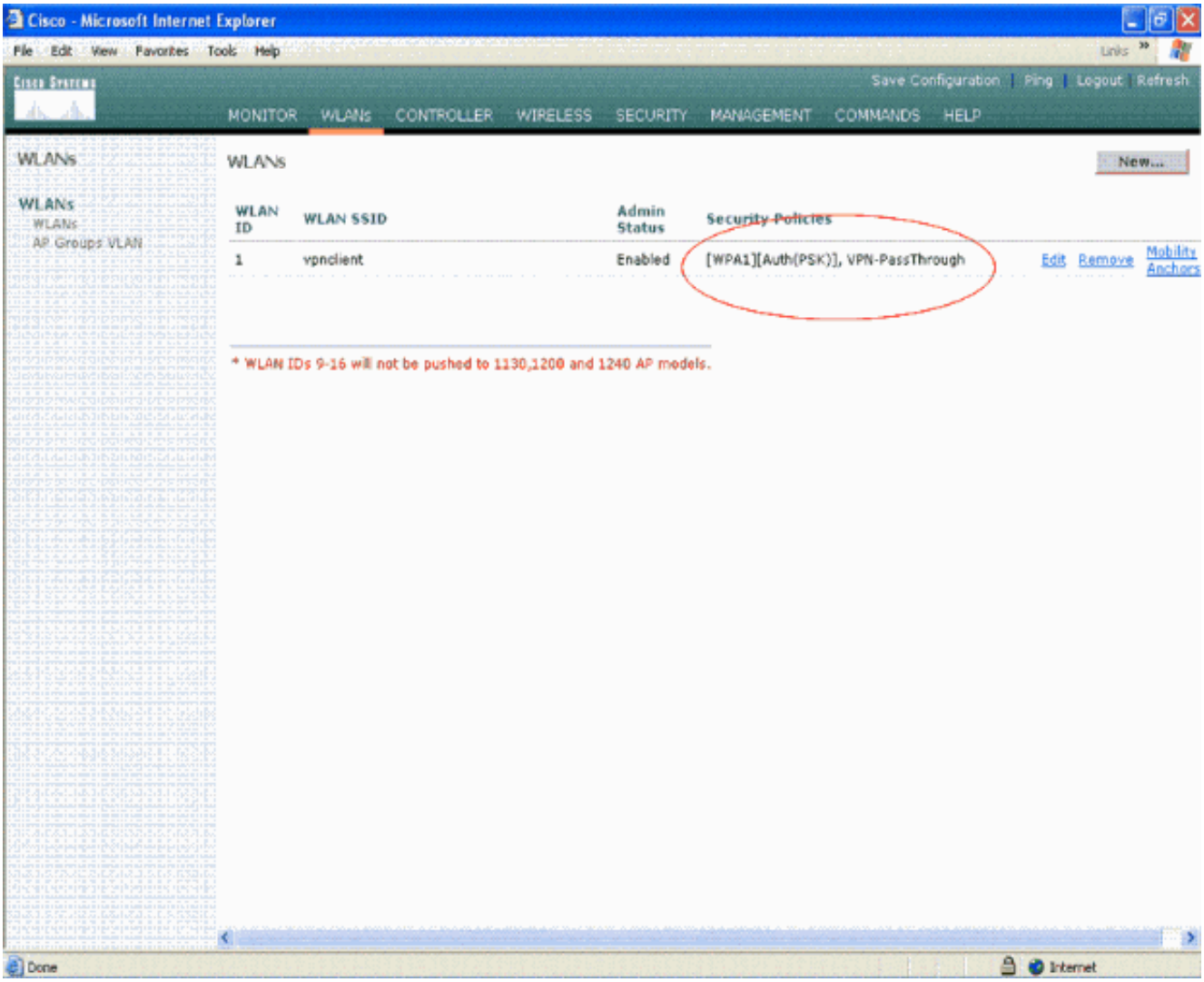
6. Selecione **VPN Pass-through** como a Segurança de Camada 3. Aqui está o exemplo.



7. Depois que a passagem de VPN for selecionada como a segurança da camada 3, adicione o endereço do gateway de VPN como mostrado neste exemplo.Esse endereço de gateway deve ser o endereço IP da interface que termina o túnel VPN no lado do servidor. Neste exemplo, o endereço IP da interface s3/0 (192.168.1.11/24) no servidor VPN é o endereço de gateway a ser
configurado.



8. Clique em Apply. A WLAN chamada *vpnclient* agora está configurada para passagem de VPN.



Configuração do Servidor VPN

Essa configuração mostra o Cisco 3640 Router como o servidor VPN.

Observação: para simplificar, essa configuração usa o roteamento estático para manter o alcance do IP entre os terminais. Você pode usar qualquer protocolo de roteamento dinâmico como o Routing Information Protocol (RIP), Open Shortest Path First (OSPF) e assim por diante para manter a acessibilidade.

Observação: o túnel não será estabelecido se não houver alcance de IP entre o cliente e o servidor.

Observação: este documento pressupõe que o usuário está ciente de como ativar o roteamento dinâmico na rede.

Cisco 3640 Router

```
vpnrouter#show running-config

Building configuration...

Current configuration : 1623 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiation. hash md5
!--- Choose the hash algorithm to be md5. authentication
pre-share
!--- The authentication method selected is pre-shared.
group 2
!--- With the group command, you can declare what size
modulus to !--- use for Diffie-Hellman calculation.
Group 1 is 768 bits long, !--- and group 2 is 1024 bits
long.


crypto isakmp client configuration group employee key
cisco123 pool mypool
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!--- Create a dynamic map and apply the transform set
that was created. !--- Set reverse-route for the VPN
server. crypto dynamic-map mymap 10 set transform-set
```

```
myset reverse-route
!
crypto map clientmap isakmp authorization list employee
!--- Create the crypto map.
crypto map clientmap client configuration address crypto
map clientmap 10 ipsec-isakmp dynamic mymap
!
!--- Apply the employee group list that was created
earlier.



!
!
!
!
interface Ethernet0/0
 ip address 10.0.0.20 255.0.0.0
 half-duplex
!
interface Serial3/0
 ip address 192.168.1.11 255.255.255.0
 clock rate 64000
 no fair-queue
 crypto map clientmap
!--- Apply the crypto map to the interface. ! interface
Serial3/1 no ip address shutdown ! interface Serial3/2
no ip address shutdown ! interface Serial3/3 no ip
address shutdown ! interface Serial3/4 no ip address
shutdown ! interface Serial3/5 no ip address shutdown !
interface Serial3/6 no ip address shutdown ! interface
Serial3/7 no ip address shutdown ip local pool mypool
10.0.0.50 10.0.0.60
!--- Configure the Dynamic Host Configuration Protocol
!--- (DHCP) pool which assigns the tunnel !--- IP
address to the wireless client. !--- This tunnel IP
address is different from the IP address !--- assigned
locally at the wireless client (either statically or
dynamically). ip http server no ip http secure-server !
ip route 172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! !
control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 ! ! end ip subnet-zero . . . ! end
```

Observação: este exemplo usa apenas a autenticação de grupo. Não usa autenticação de usuário individual.

Configuração de cliente de VPN

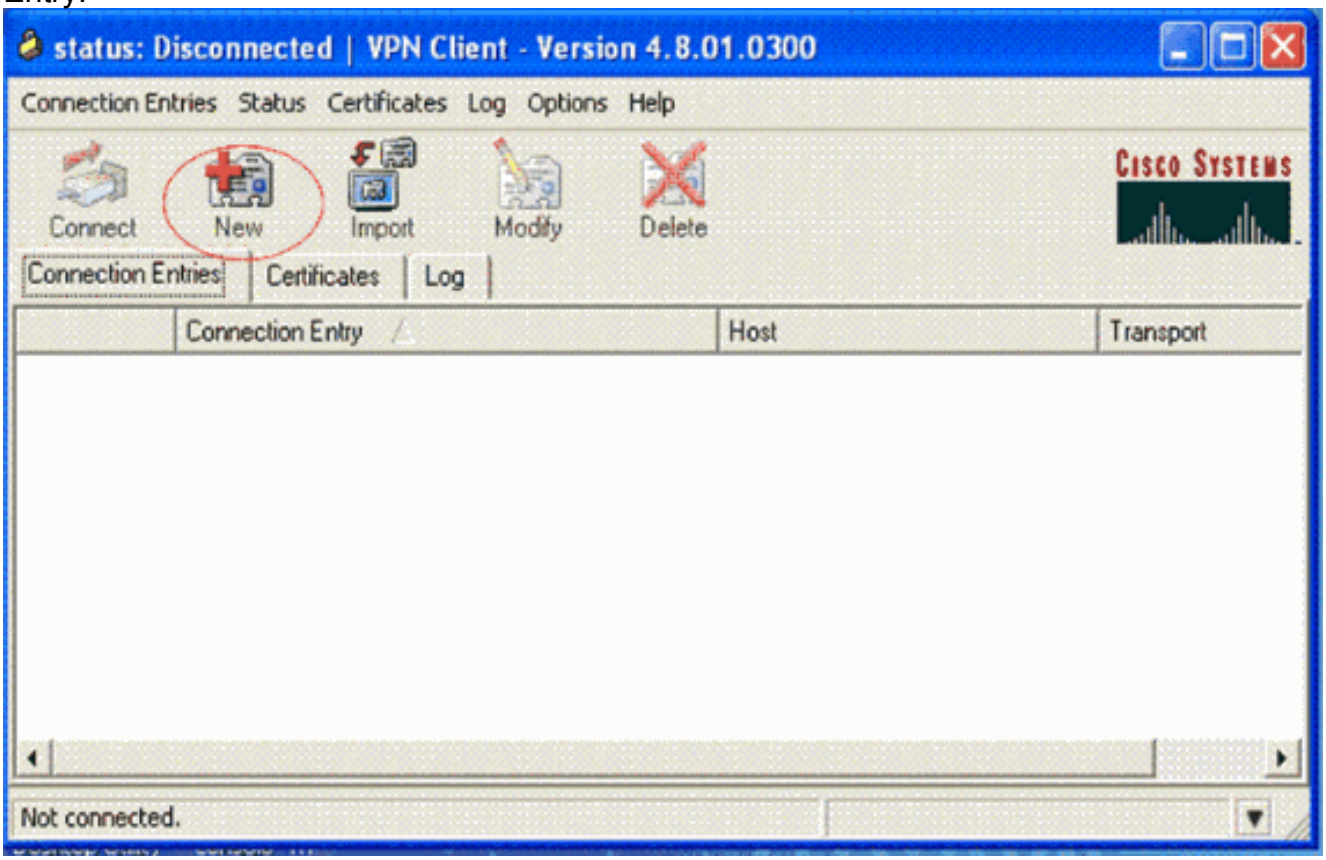
Um software VPN Client pode ser baixado do Cisco.com Software Center.

Observação: alguns softwares da Cisco exigem que você faça login com um nome de usuário e uma senha do CCO.

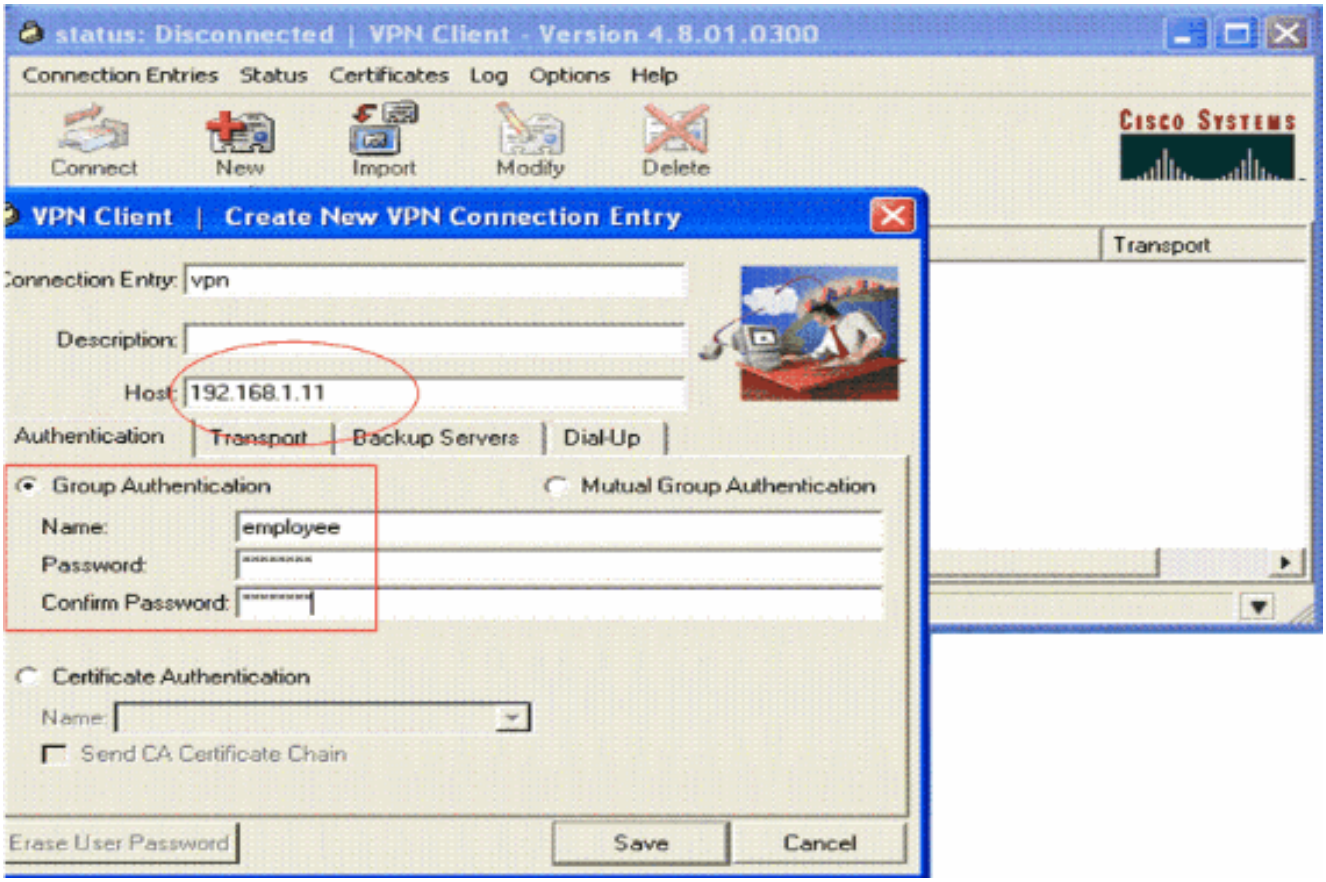
Conclua estes passos para configurar o VPN Client.

1. De seu cliente sem fio (laptop), escolha **Iniciar > Programas > Cisco Systems VPN Client > VPN Client** para acessar o VPN Client. Esse é o local padrão onde o VPN Client está instalado.
2. Clique em **New** para iniciar a janela Create New VPN Connection

Entry.



3. Insira o nome da entrada do Connection junto com uma descrição. Este exemplo *usa vpn*.O campo Descrição é opcional. Digite o endereço IP do servidor VPN na caixa Host. Em seguida, insira o nome do grupo VPN e a senha e clique em **Salvar**.



Observação: o nome do grupo e a senha configurados aqui devem ser os mesmos configurados no servidor VPN. Este exemplo usa o Nome do *funcionário* e a Senha

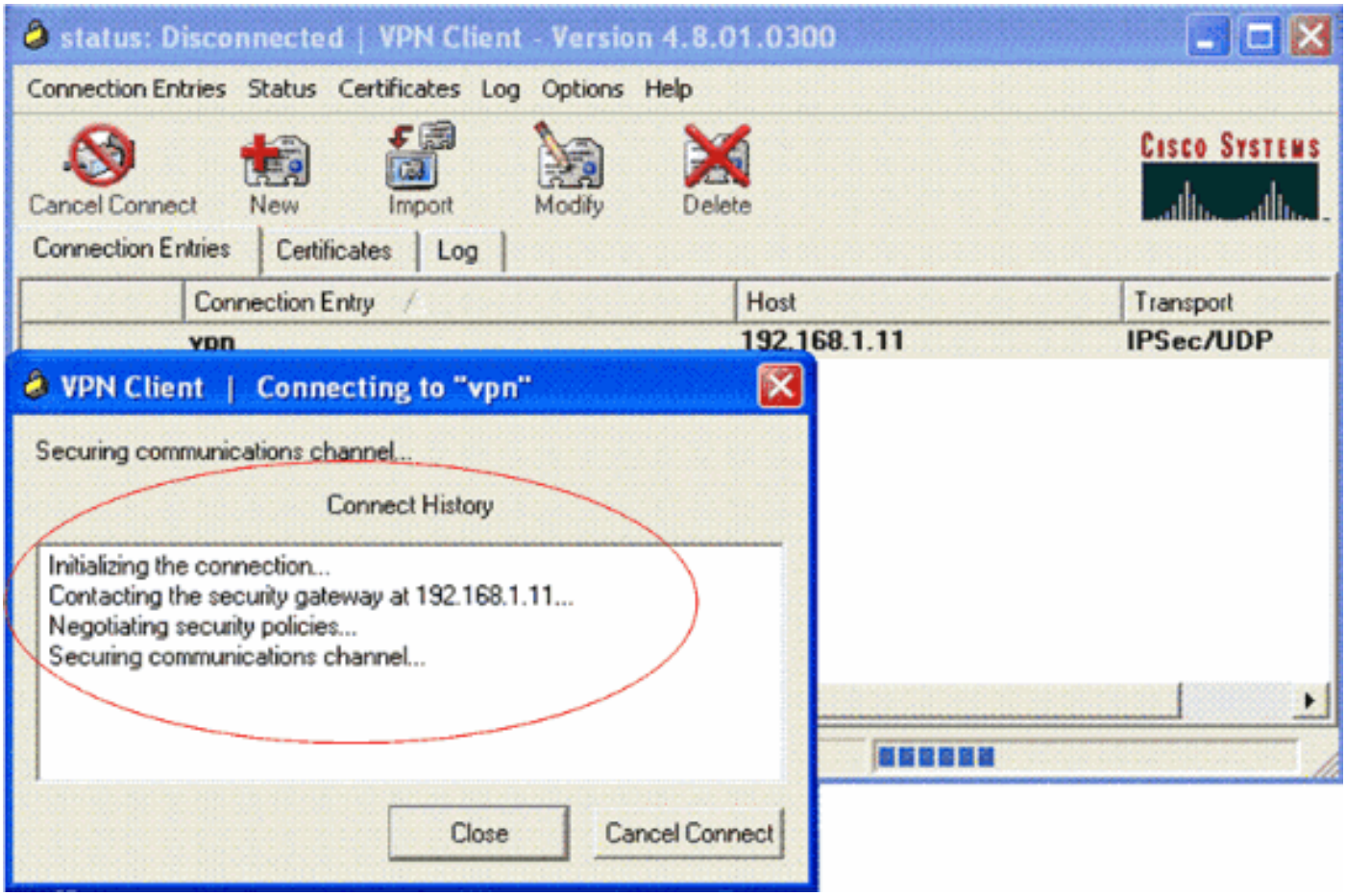
cisco123.

Verificar

Para verificar essa configuração, configure o SSID **vpnclient** no cliente sem fio com os mesmos parâmetros de segurança configurados na WLC e associe o cliente a essa WLAN. Há vários documentos que explicam como configurar um cliente sem fio com um novo perfil.

Quando o cliente sem fio estiver associado, vá para o VPN Client e clique na conexão configurada. Em seguida, clique em **Connect** na janela principal do VPN Client.

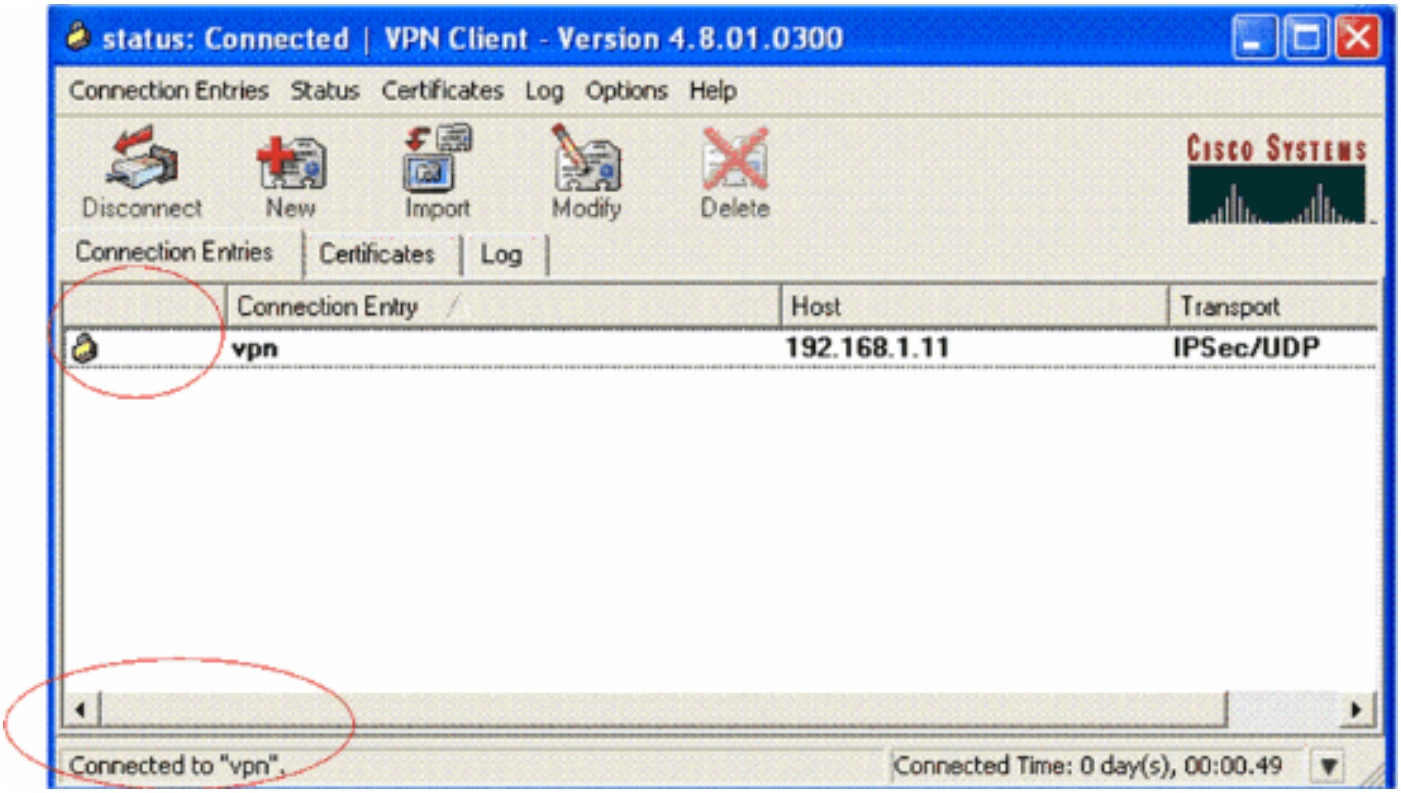
Você pode ver os parâmetros de segurança de Fase 1 e Fase 2 negociados entre o cliente e o servidor.



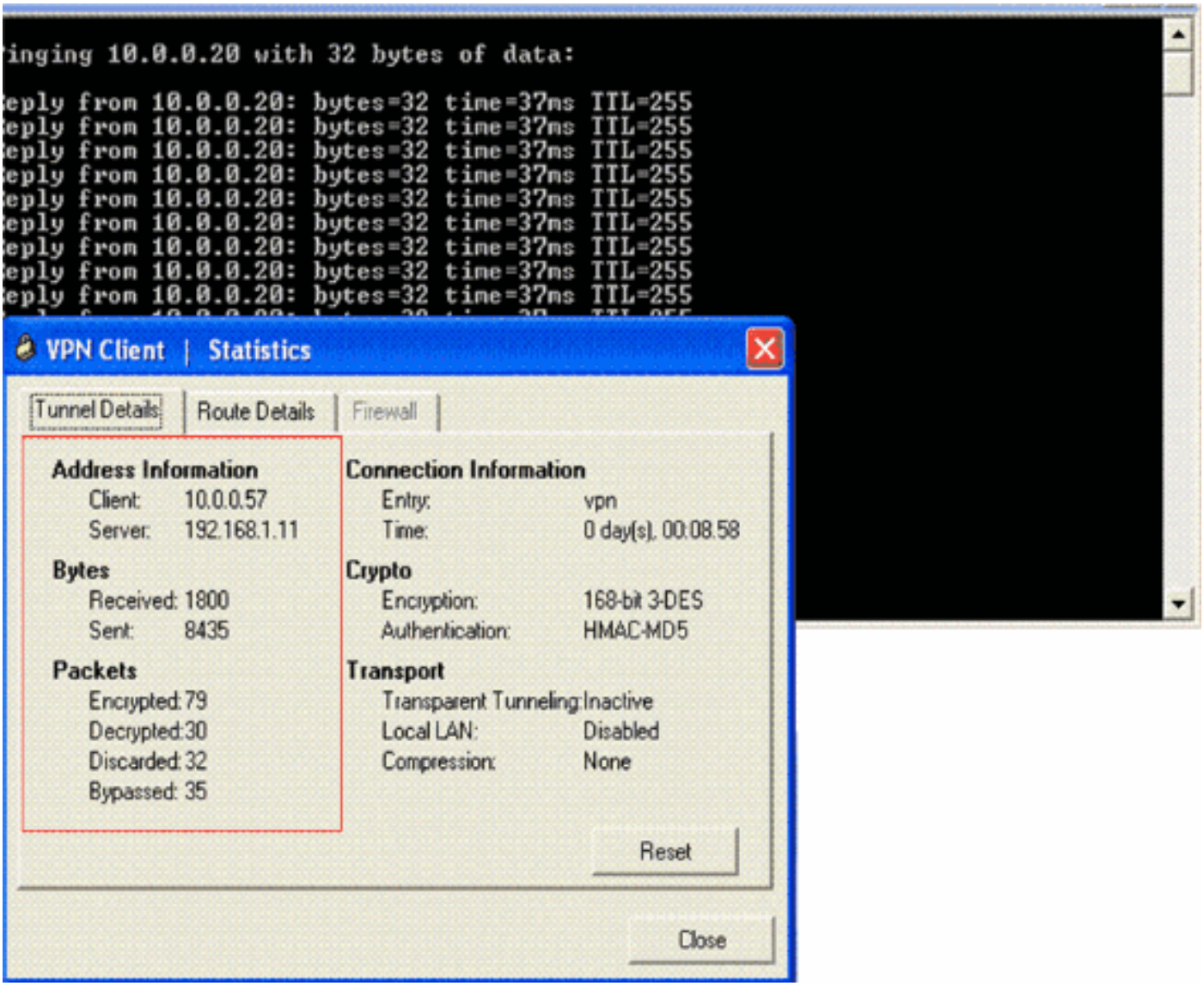
Observação: para estabelecer esse túnel VPN, o VPN Client e o servidor devem ter alcance de IP entre eles. Se o VPN Client não puder entrar em contato com o gateway de segurança (servidor VPN), o túnel não será estabelecido e uma caixa de alerta será exibida no lado do cliente com esta mensagem:

```
Reason 412: The remote peer is no longer responding
```

Para garantir que um túnel VPN seja estabelecido corretamente entre o cliente e o servidor, você pode encontrar um ícone de bloqueio criado ao lado do VPN Client estabelecido. A barra de status também indica **Connected to "vpn"**. Exemplo:



Além disso, certifique-se de que você possa transmitir dados para o segmento da LAN com êxito no lado do servidor do VPN Client e vice-versa. No menu principal do VPN Client, escolha **Status > Statistics**. Lá você pode encontrar as estatísticas dos pacotes criptografados e descriptografados que são passados pelo túnel.



Nesta captura de tela, você pode ver o endereço do cliente como 10.0.0.57. Esse é o endereço que o servidor VPN atribui ao cliente de seu pool configurado localmente após a negociação bem-sucedida da Fase 1. Quando o túnel é estabelecido, o servidor VPN adiciona automaticamente uma rota a esse endereço IP DHCP atribuído em sua tabela de rotas.

Você também pode ver o número de pacotes criptografados aumentando enquanto os dados são transferidos do cliente para o servidor e o número de pacotes descriptografados aumentando durante uma transferência de dados reversa.

Observação: como a WLC está configurada para VPN Pass-through, ela permite que o cliente acesse somente o segmento conectado ao gateway VPN (aqui, é o servidor VPN 192.168.1.11) configurado para Pass-through. Isso filtra todo o tráfego restante.

Você pode verificar isso configurando outro servidor VPN com a mesma configuração e configurando uma nova entrada de conexão para esse servidor VPN no VPN Client. Agora, quando você tenta estabelecer um túnel com esse servidor VPN, ele não é bem-sucedido. Isso ocorre porque a WLC filtra esse tráfego e permite um túnel somente para o endereço do gateway VPN configurado para passagem de VPN.

Você também pode verificar a configuração a partir da CLI do servidor VPN.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a 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.

Esses comandos **show** usados no servidor VPN também podem ser úteis para ajudar você a verificar o status do túnel.

- O comando **show crypto session** é usado para verificar o status do túnel. Aqui está um exemplo de saída desse comando.

```
Crypto session current status

Interface: Serial3/0
Session status: UP-ACTIVE
Peer: 172.16.1.20 port 500
  IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58
        Active SAs: 2, origin: dynamic crypto map
```

- A **política show crypto isakmp** é usada para exibir os parâmetros configurados da Fase 1.

Troubleshoot

Os comandos **debug** e **show** explicados na seção Verify também podem ser usados para solucionar problemas.

- **debug crypto isakmp**
- **debug crypto ipsec**
- **show crypto session**

- O comando **debug crypto isakmp** no servidor VPN exibe todo o processo de negociação da Fase 1 entre o cliente e o servidor. Aqui está um exemplo de uma negociação bem-sucedida da Fase 1.

```
------------------------------------------------------------------
 ----------------------------------------------------------
------------------------------------------------------------
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14
   against priority 1 policy
*Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC
*Aug 28 10:37:29.515: ISAKMP:      hash MD5
*Aug 28 10:37:29.515: ISAKMP:      default group 2
*Aug 28 10:37:29.515: ISAKMP:      auth pre-share
*Aug 28 10:37:29.515: ISAKMP:      life type in seconds
*Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Aug 28
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA authentication status:
authenticated
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact,
  bring down existing phase 1 and 2 SA's with local 192.168.1.11
  remote 172.16.1.20 remote port 500
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
  the address pool: 10.0.0.57
*Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool
```

```
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade
  1583442981 to QM_IDLE
*Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY
  RESPONDER_LIFETIME protocol 1
spi 1689265296, message ID = 1583442981
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to
  172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981
*Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400

*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2
  New State = IKE_P1_COMPLETE
```

- O comando **debug crypto ipsec** no servidor VPN exibe a negociação IPsec de fase 1 bem-sucedida e a criação do túnel VPN. Aqui está um exemplo:

```
----------------------------------------------------------------------
 ----------------------------------------------------------------
----------------------------------------------------------------------
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for
  peer or rekeying for peer 172.16.1.20
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added
  10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0
*Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F
*Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58,
  dest_port 0

*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.11, sa_proto= 50,
    sa_spi= 0x8538A817(2235082775),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.20, sa_proto= 50,
    sa_spi= 0xFFC80936(4291299638),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

Informações Relacionadas

- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)

- Página do suporte de protocolo do IPsec Negotiation/IKE
- Configuração da segurança de rede IPSec
- Perguntas e respostas sobre o Cisco Easy VPN
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Exemplo de configuração de ACLs em Wireless LAN Controller
- Perguntas frequentes sobre o Wireless LAN Controller (WLC)
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.