Cliente VPN sobre LAN Wireless com Exemplo de Configuração de WLC

Índice

Introdução

Este documento introduz o conceito do Virtual Private Network (VPN) em um ambiente Wireless. O documento explica as configurações envolvidas no desenvolvimento de um túnel VPN entre um cliente Wireless e um servidor de VPN através de um controlador do Wireless LAN (WLC).

Pré-requisitos

Requisitos

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

- Conhecimento dos WLC e como configurar os parâmetros básicos WLC
- Conhecimento de conceitos do Wi-Fi Protected Access (WPA)
- Conhecimento básico do VPN e dos seus tipos
- Conhecimento do IPsec
- Conhecimento básico da criptografia, da autenticação e dos algoritmos de hashing 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 de pouco peso do Cisco 1000 Series (REGAÇO)
- Cisco 3640 que executa a liberação do Cisco IOS ® Software 12.4(8)
- Versão Cliente VPN Cisco 4.8

Nota: Este documento usa um 3640 Router como um servidor de VPN. A fim apoiar mais recursos de segurança avançada, você pode igualmente usar um servidor de VPN dedicado.

Nota: Para que um roteador atue como um servidor de VPN, precisa de executar um conjunto de recursos que apoie o IPsec básico.

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.

Informações de Apoio

Um VPN é uma rede de dados privados que seja usada para transmitir firmemente os dados dentro de uma rede privada através da infraestrutura de telecomunicação pública tal como o Internet. Este VPN mantém a privacidade de dados com o uso de um protocolo de tunelamento e de procedimentos de segurança.

Acesso remoto VPN

Uma configuração do acesso remoto VPN é usada para permitir que os clientes do software de VPN tais como usuários móveis alcancem firmemente os recursos de rede centralizada que residem atrás de um servidor de VPN. Nas terminologias Cisco, estes servidores de VPN e clientes são chamados igualmente o server do Cisco Easy VPN e o dispositivo remoto do Cisco Easy VPN.

Um dispositivo remoto do Cisco Easy VPN pode ser Roteadores do Cisco IOS, ferramentas de segurança de Cisco PIX, Cisco VPN 3002 Hardware Client e o Cisco VPN Client. São usados para receber políticas de segurança em cima de uma conexão de túnel VPN de um server do Cisco Easy VPN. Isto minimiza requisitos de configuração na posição remota. O Cisco VPN Client é um cliente de software que possa ser instalado em PC, portáteis, e assim por diante.

Um server do Cisco Easy VPN pode ser Roteadores do Cisco IOS, ferramentas de segurança de Cisco PIX, e concentradores do Cisco VPN 3000.

Este documento usa o software Cisco VPN Client que é executado em um portátil como o cliente VPN e o IOS Router do Cisco 3640 como o servidor de VPN. O documento usa o padrão do

IPsec para estabelecer um túnel VPN entre um cliente e um server.

IPsec

O IPsec é uma estrutura dos padrões abertos desenvolvidos pelo Internet Engineering Task Force (IETF). O IPsec fornece a Segurança para a transmissão da informação sensível sobre redes desprotegidas tais como o Internet.

O IPsec fornece a criptografia de dados de rede a nível do pacote IP, que oferece uma solução de segurança robusta que seja com base em padrões. As tarefas principal do IPsec são permitir a troca da informação privada sobre uma conexão incerta. O IPsec usa a criptografia para proteger a informação da intercepção ou de bisbilhotar. Contudo, para usar eficientemente a criptografia, ambos os partidos devem compartilhar de um segredo que seja usado para a criptografia e a descriptografia da informação.

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

- Fase 1 — Segura a negociação dos parâmetros de segurança exigidos estabelecer um canal seguro entre dois ipsec peer. A fase 1 é executada geralmente com o protocolo do Internet Key Exchange (IKE). Se o ipsec peer remoto não pode executar o IKE, você pode usar a configuração manual com chaves pré-compartilhada para terminar a fase 1.
- Fase 2 — Usa o túnel seguro estabelecido na fase 1 para trocar os parâmetros de segurança exigidos para transmitir realmente dados do usuário. Os túneis seguros usados em ambas as fases de IPsec são baseados nas associações de segurança (SA) usadas em cada ponto final do IPsec. Os SA descrevem os parâmetros de segurança, tais como o tipo de autenticação e de criptografia que ambos os pontos finais concordam usar.

Os parâmetros de segurança trocados na fase 2 são usados para criar um túnel de IPsec que seja usado por sua vez para transferência de dados entre o cliente VPN e o server.

Refira configurar o IPsec para obter mais informações sobre do IPsec e da sua configuração.

Uma vez que um túnel VPN é estabelecido entre o cliente VPN e o server, as *políticas de segurança definidas no servidor de VPN estão enviadas ao cliente*. Isto minimiza requisitos de configuração no lado do cliente.

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

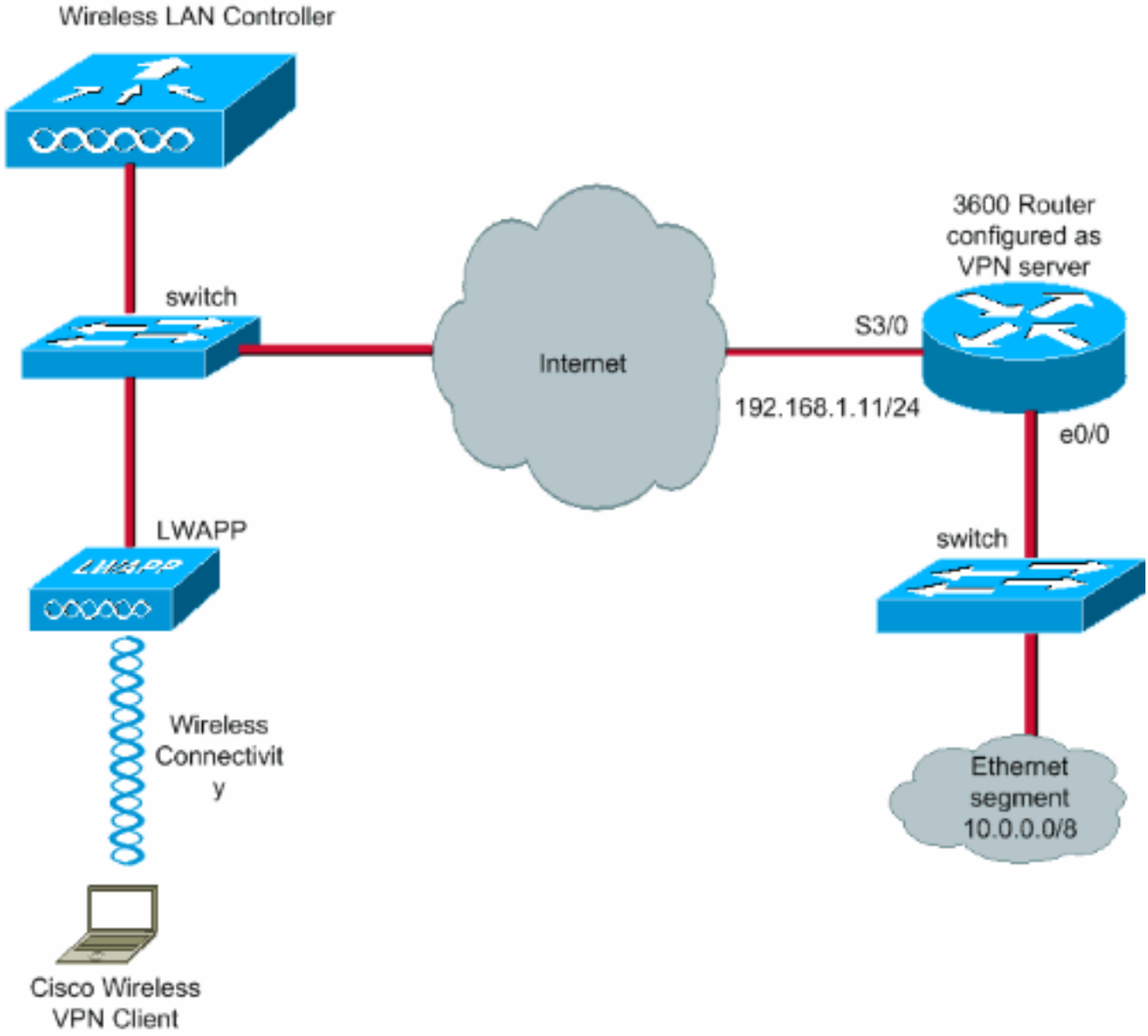
Diagrama de Rede

Este documento utiliza as seguintes configurações:

- Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do WLC — 172.16.1.10/16
- Endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do gerenciador AP do WLC — 172.16.1.11/16
- Gateway padrão — 172.16.1.20/16**Nota:** Em uma rede viva, este gateway padrão deve apontar à interface de entrada do roteador imediato que conecta o WLC ao resto da rede e/ou ao Internet.
- Endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de VPN s3/0 —

192.168.1.11/24**Nota:** Este endereço IP de Um ou Mais Servidores Cisco ICM NT deve apontar à relação que termina o túnel VPN no lado do servidor de VPN. Neste exemplo, s3/0 é a relação que termina o túnel VPN no servidor de VPN.

- O segmento de LAN no servidor de VPN usa o intervalo de endereço IP de 10.0.0.0/8.



Configurar

Em um WLAN arquitetura centralizada, a fim permitir que um cliente VPN wireless tal como um portátil estabeleça um túnel VPN com um servidor de VPN, é necessário que o cliente obtém associado com um Access point de pouco peso (REGAÇO) que por sua vez necessidades de ser registrado com um WLC. Este documento tem o REGAÇO como já registrado com o WLC usando o processo de descoberta da transmissão da sub-rede local explicado no registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (WLC).

A próxima etapa é configurar o WLC para o VPN.

Terminação VPN e Passagem-através de

Com Cisco 4000 Series WLC mais cedo do que a versão 4, uma característica chamada terminação do IPSec VPN (suporte de IPSec) é apoiada. Esta característica permite estes

controladores de terminar sessões de cliente VPN diretamente no controlador. Em resumo, esta característica permite o controlador própria de atuar como um servidor de VPN. Mas isto exige um módulo de hardware separado da terminação VPN ser instalado no controlador.

Este apoio do IPSec VPN não está disponível em:

- Cisco 2000 Series WLC
- Alguns WLC que executarem a versão 4.0 ou mais recente

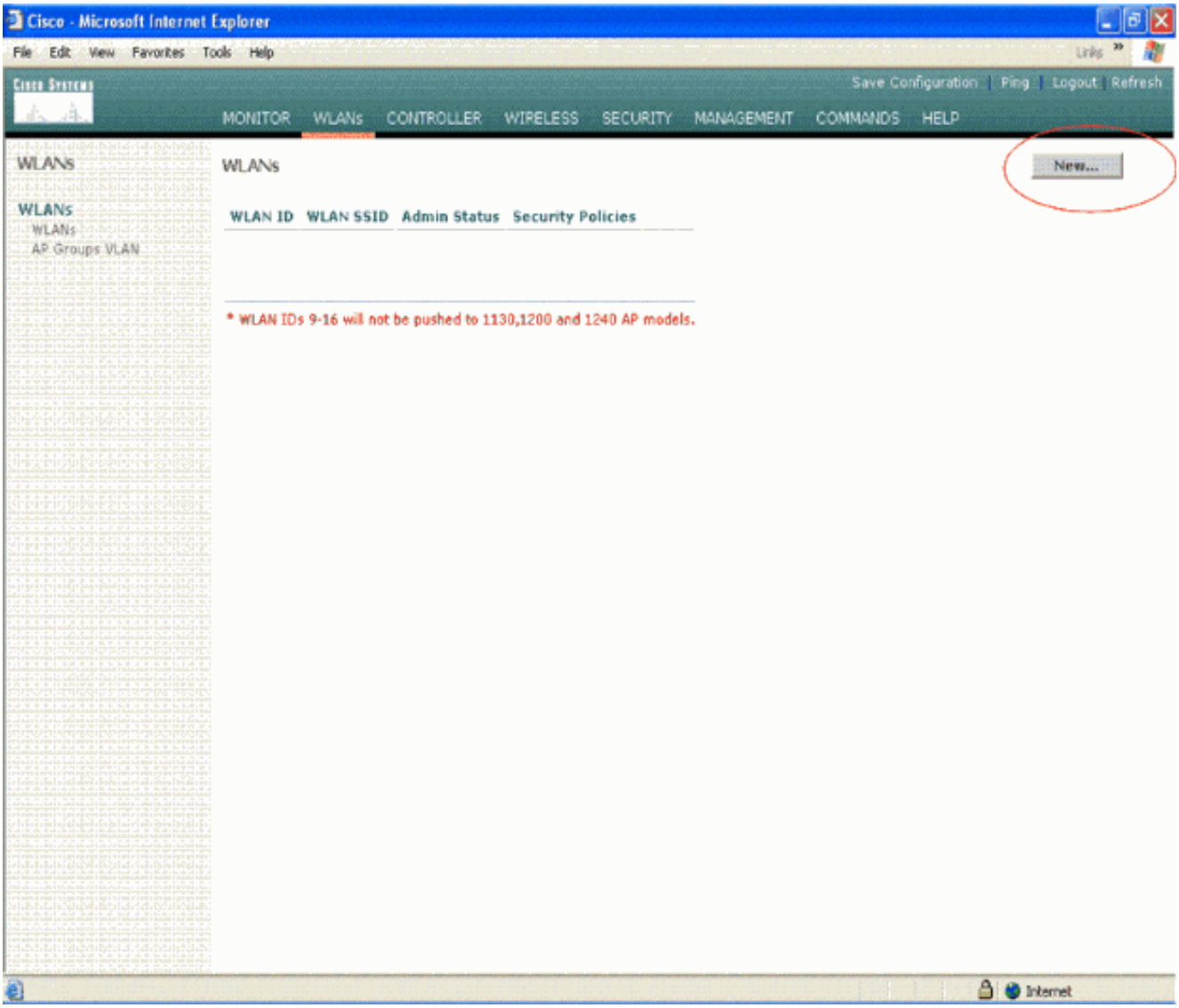
Consequentemente, a única característica VPN apoiada nas versões mais tarde de 4.0 é VPN Passagem-através de. Esta característica é apoiada igualmente no Cisco 2000 Series WLC.

O VPN Passagem-através de é uma característica que permita que um cliente estabeleça um túnel somente com um servidor de VPN específico. Assim, se você precisa de alcançar firmemente o servidor de VPN configurado assim como um outro servidor de VPN ou o Internet, isto não é possível com o VPN Passagem-através do permitido no controlador. Sob tais exigências, você precisa de desabilitar o VPN Passagem-através de. Contudo, o WLC pode ser configurado para atuar como a transmissão a fim alcançar gateways de VPN múltiplos quando um ACL apropriado é criado e aplicado ao WLAN correspondente. Assim, sob tais encenações onde você quer alcançar gateways de VPN múltiplos para a Redundância, desabilita a transmissão VPN e cria um ACL que permita o acesso aos gateways de VPN e aplica o ACL ao WLAN.

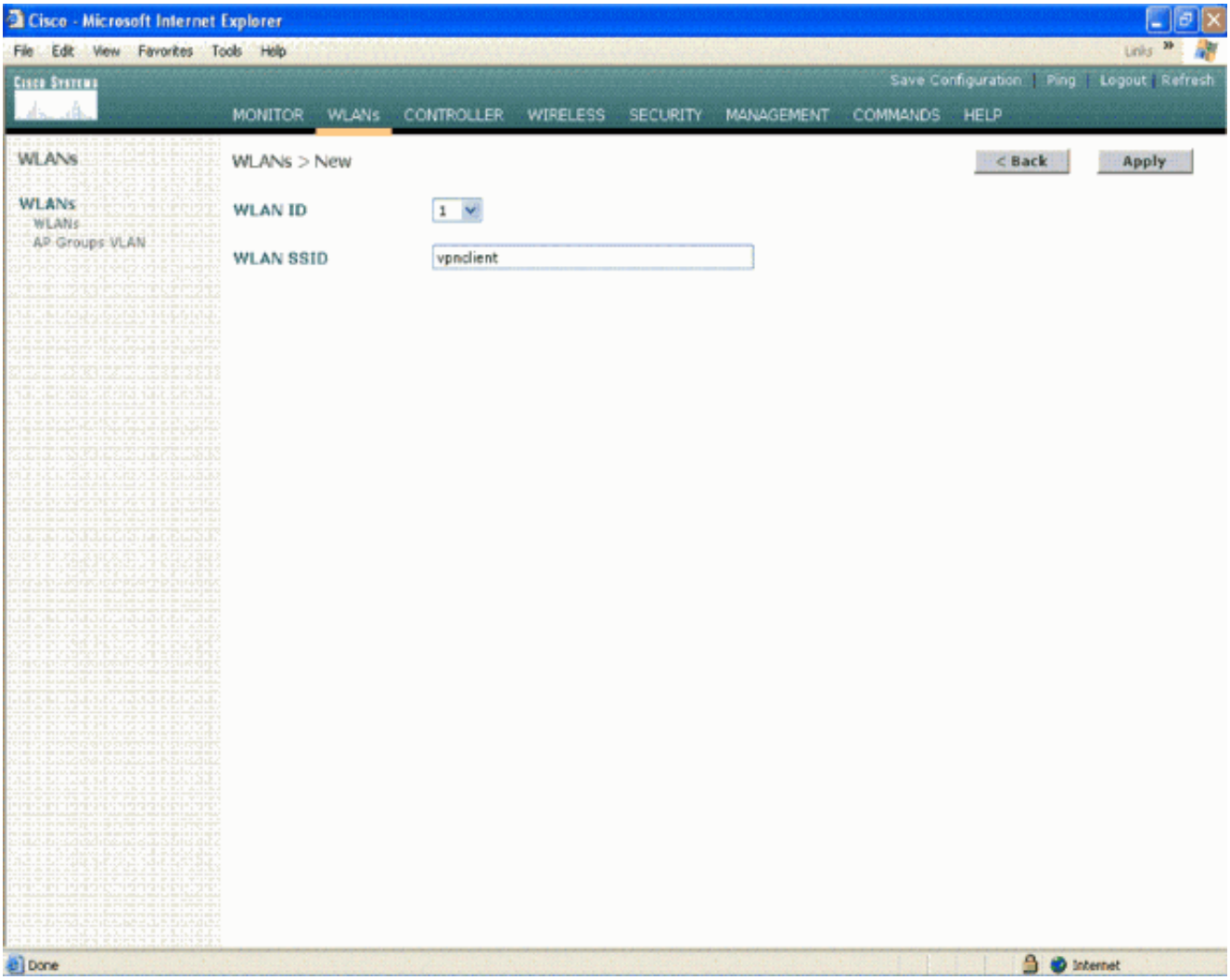
Configurar o WLC para o VPN Passagem-através de

Termine estas etapas a fim configurar o VPN Passagem-através de.

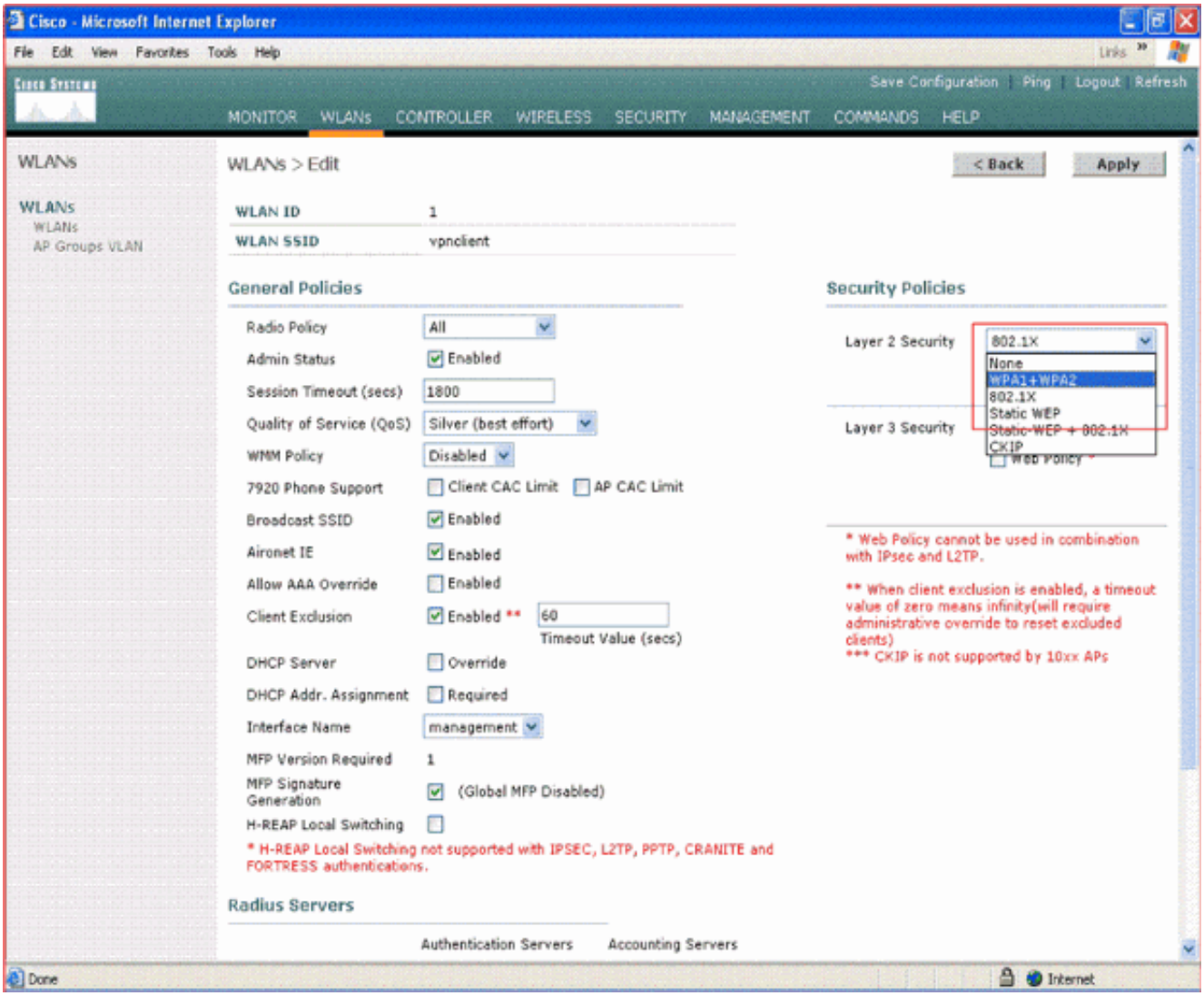
1. Do WLC GUI, clique o **WLAN** a fim ir à página WLAN.
2. Clique **novo** a fim criar um WLAN
   novo.



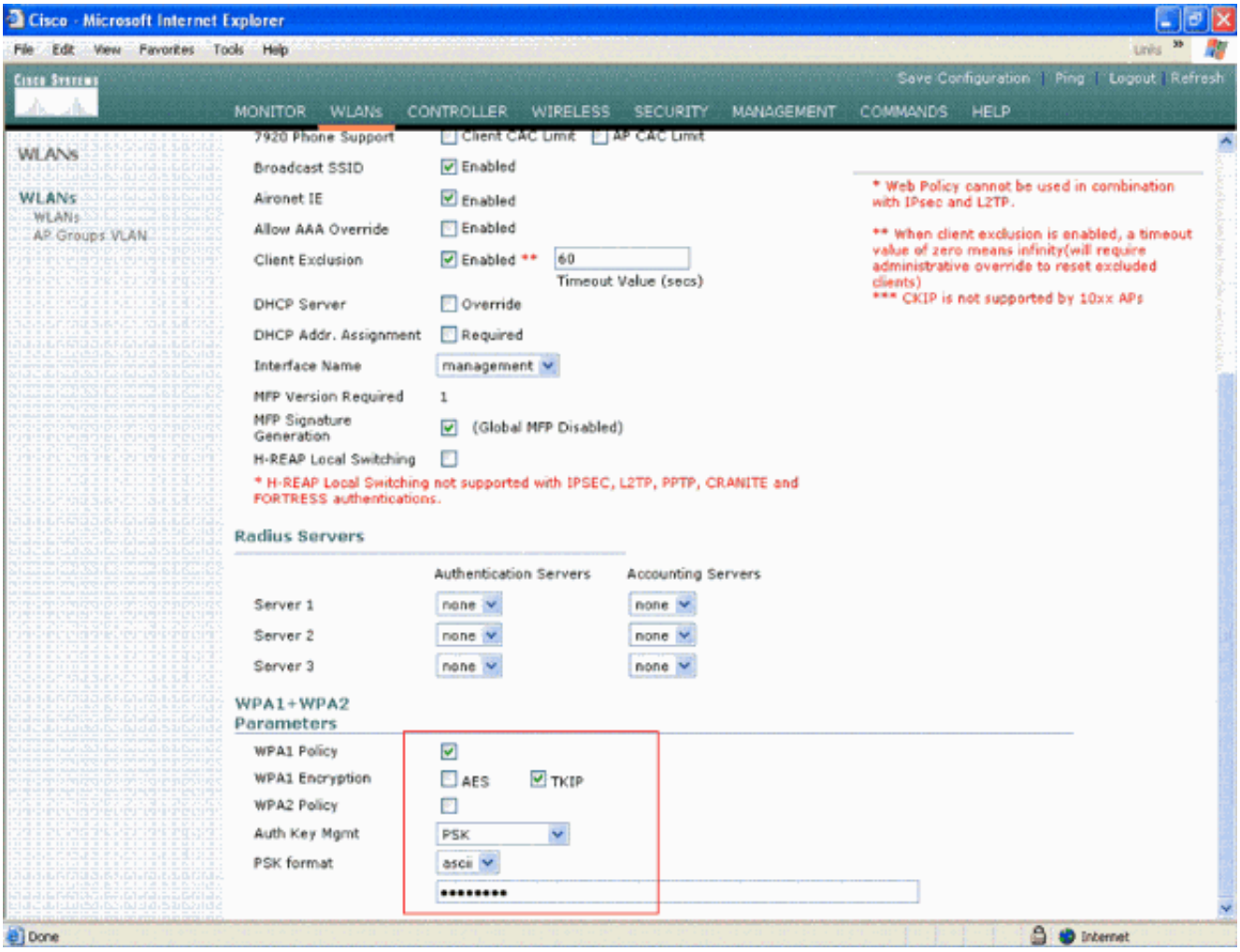
3. O WLAN SSID é nomeado como **vpnclient n**este exemplo. Clique em Apply.



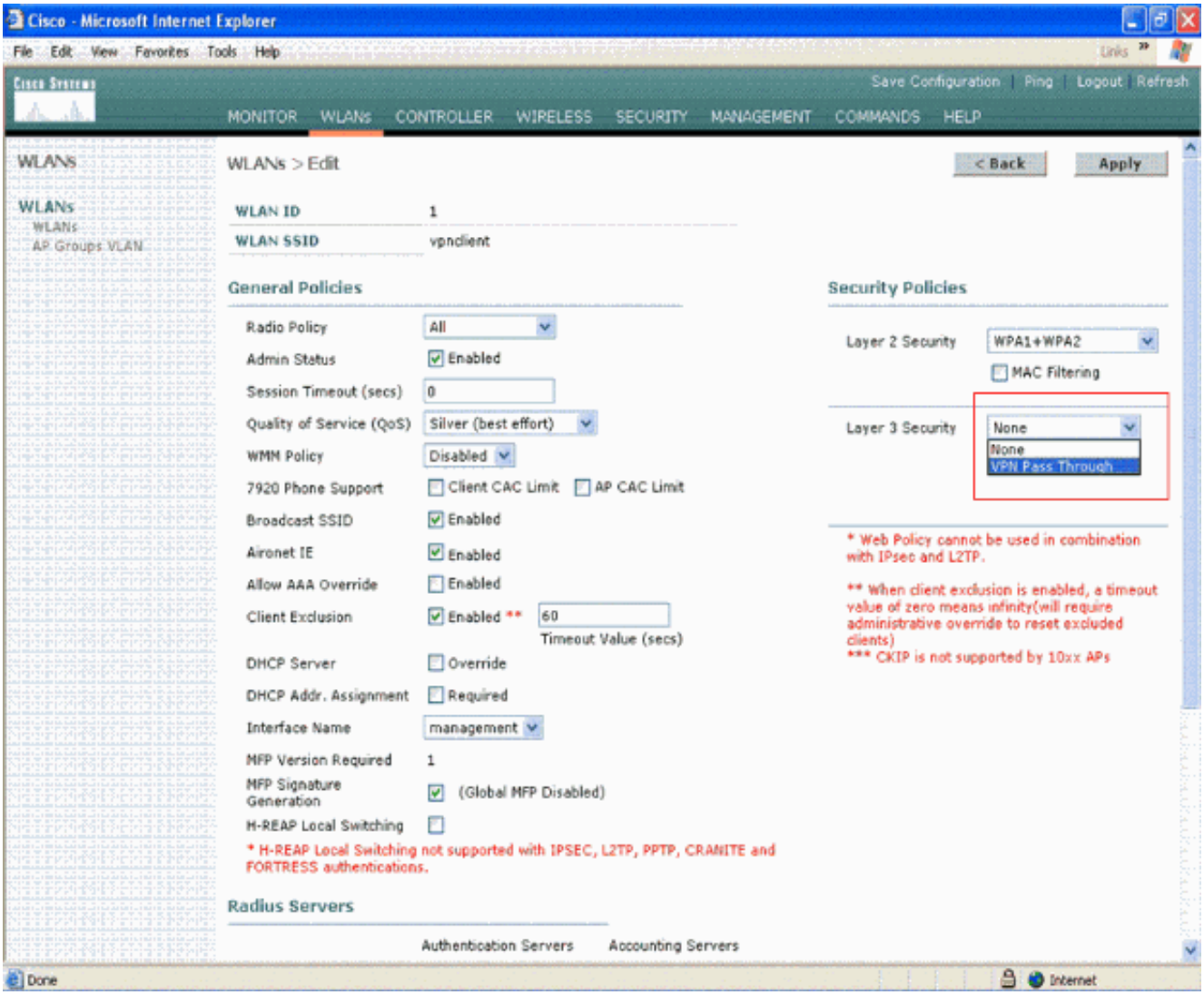
4. Configurar o SSID vpnclient com Segurança da camada 2. *Isto é opcional.*Este exemplo usa **WPA1+WPA2** como o tipo da
Segurança.



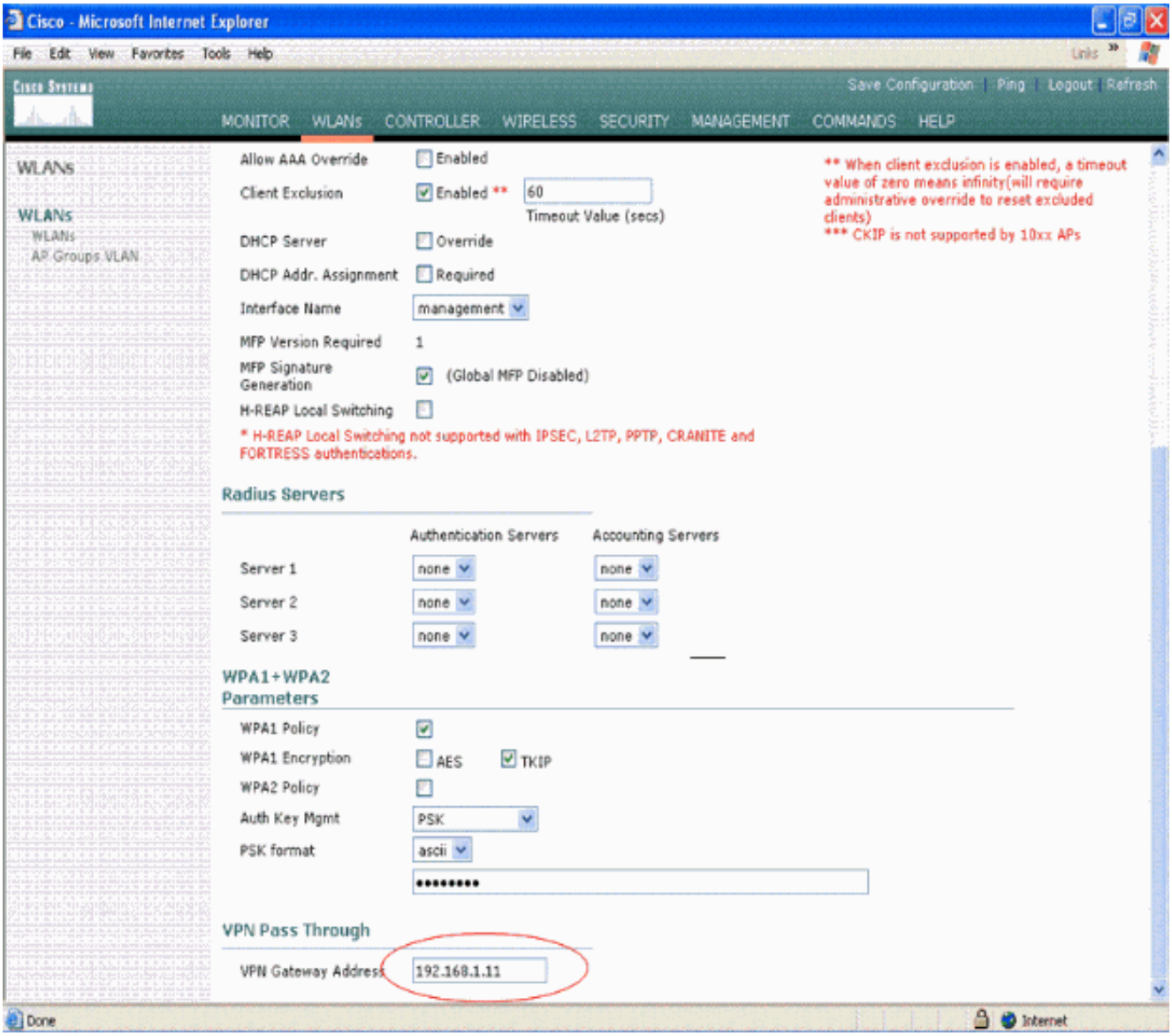
5. Configurar a política WPA e o tipo do Gerenciamento de chave de autenticação a ser usados.Este exemplo usa a **chave pré-compartilhada (PSK)** para o Gerenciamento de chave de autenticação. Uma vez que o PSK é selecionado, o **ASCII** seleto como o formato PSK e datilografa o valor PSK. Este valor deve ser o mesmo na configuração SSID do cliente Wireless para que os clientes que pertencem a este SSID para associar com este WLAN.



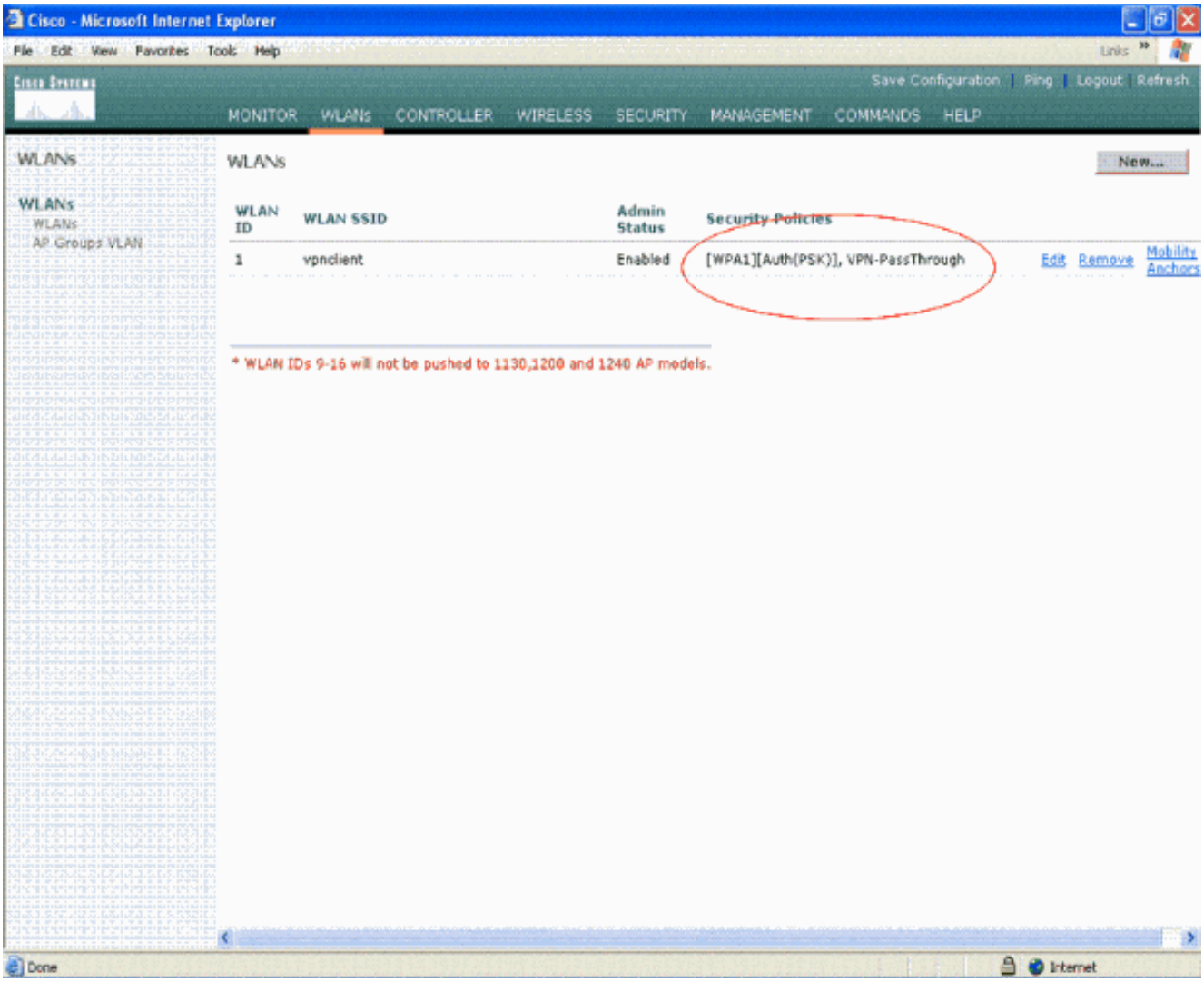
6. Selecione o **VPN Passagem-através** como da Segurança da camada 3. Está aqui o exemplo.



7. Uma vez que o VPN Passagem-através de é selecionado como a Segurança da camada 3, adicionar o endereço do gateway de VPN como este exemplo mostra.Este endereço de gateway deve ser o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação que termina o túnel VPN no lado de servidor. Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação s3/0 (192.168.1.11/24) no servidor de VPN é o endereço de gateway a ser
configurado.



8. Clique em Apply. O WLAN chamado *vpnclient* é configurado agora para o VPN Passagem-através
de.



Configuração de servidor de VPN

Esta configuração mostra o Cisco 3640 Router como o servidor de VPN.

Nota: Para a simplicidade, esta configuração usa o roteamento estático para manter o IP reachability entre os pontos finais. Você pode usar todo o protocolo de roteamento dinâmico tal como o Routing Information Protocol (RIP), Open Shortest Path First (OSPF), e assim por diante para manter a alcançabilidade.

Nota: O túnel não é estabelecido se não há nenhum IP reachability entre o cliente e o server.

Nota: Este documento supõe que o usuário está ciente de como permitir 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
```

Nota: Este exemplo usa somente a autenticação do grupo. Não usa a autenticação de usuário individual.

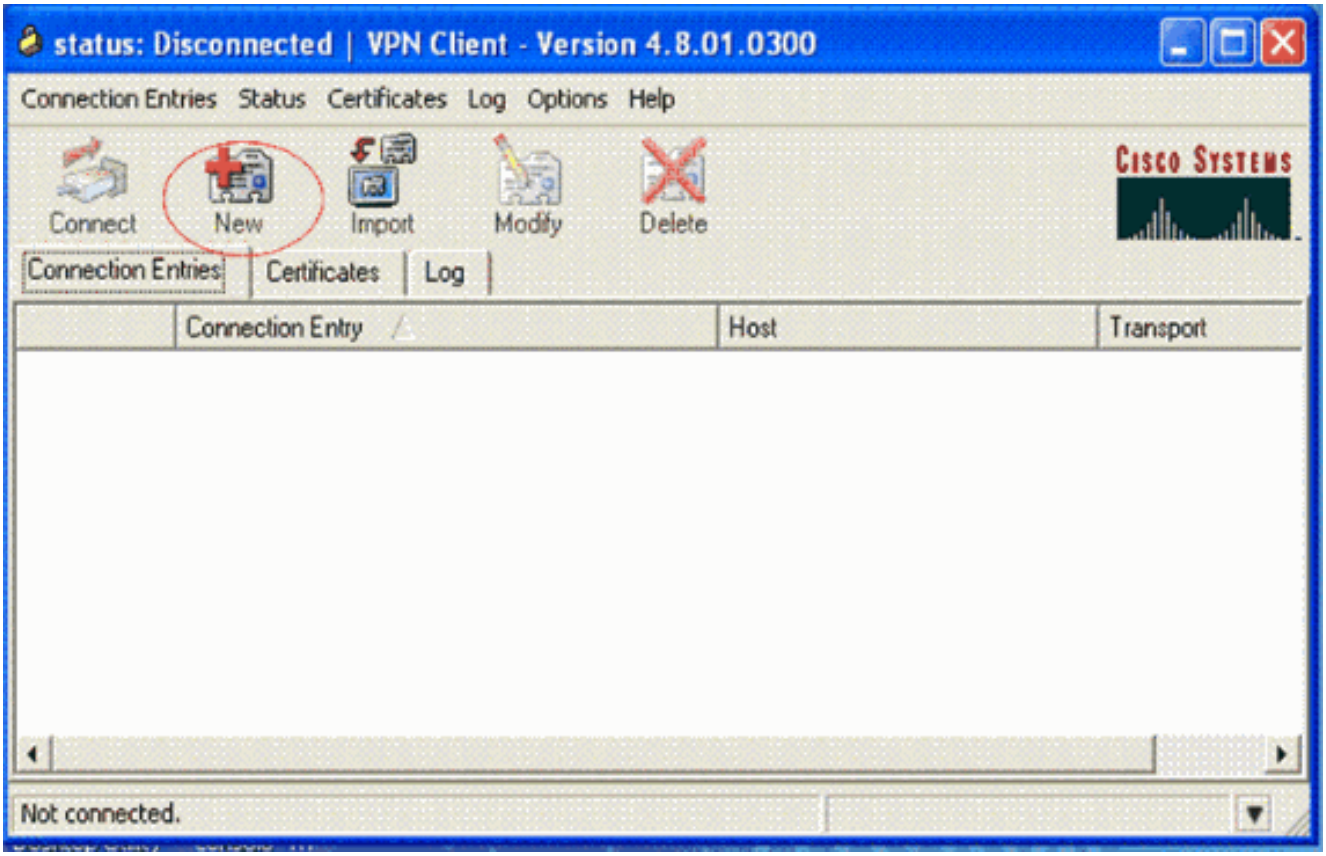
Configuração de cliente de VPN

Um cliente VPN do software pode ser transferido do centro do software da Cisco.com.

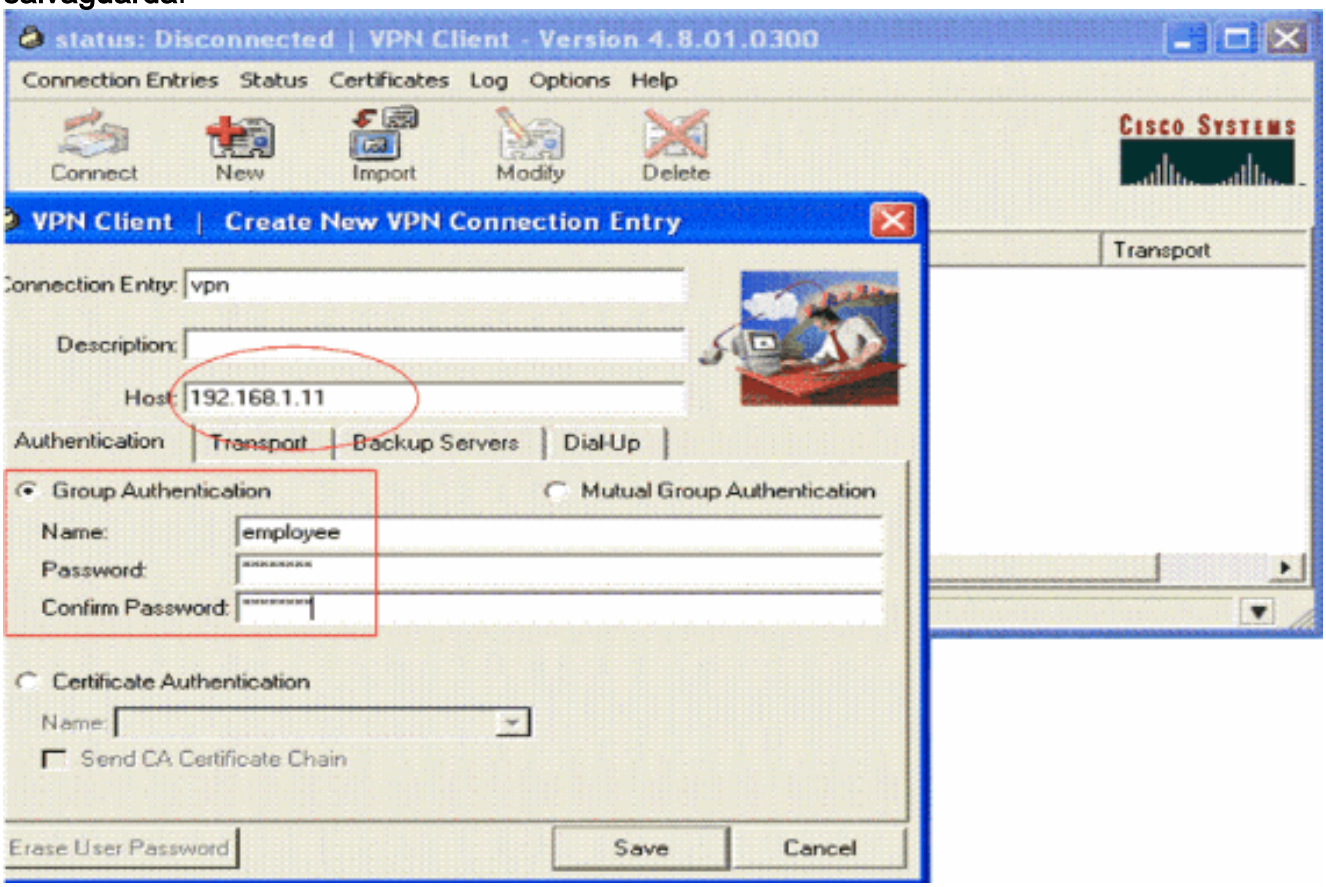
Nota: Algum software Cisco exige-o entrar com um nome de usuário e senha CCO.

Termine estas etapas a fim configurar o cliente VPN.

1. Forme seu cliente Wireless (portátil), escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN** a fim alcançar o cliente VPN. Este é o local padrão onde o cliente VPN é instalado.
2. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.



3. Dê entrada com o nome da entrada de conexão junto com uma descrição. Este usesvpn do exemplo.O campo de descrição é opcional. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de VPN à caixa do host. Então incorpore o nome do grupo VPN e a senha e clique a **salvaguarda**.



Nota: O nome do grupo e a senha configurados aqui devem ser o mesmo que esse configurado no servidor de VPN. Este exemplo usa o *empregado do* nome e o *cisco123 da*

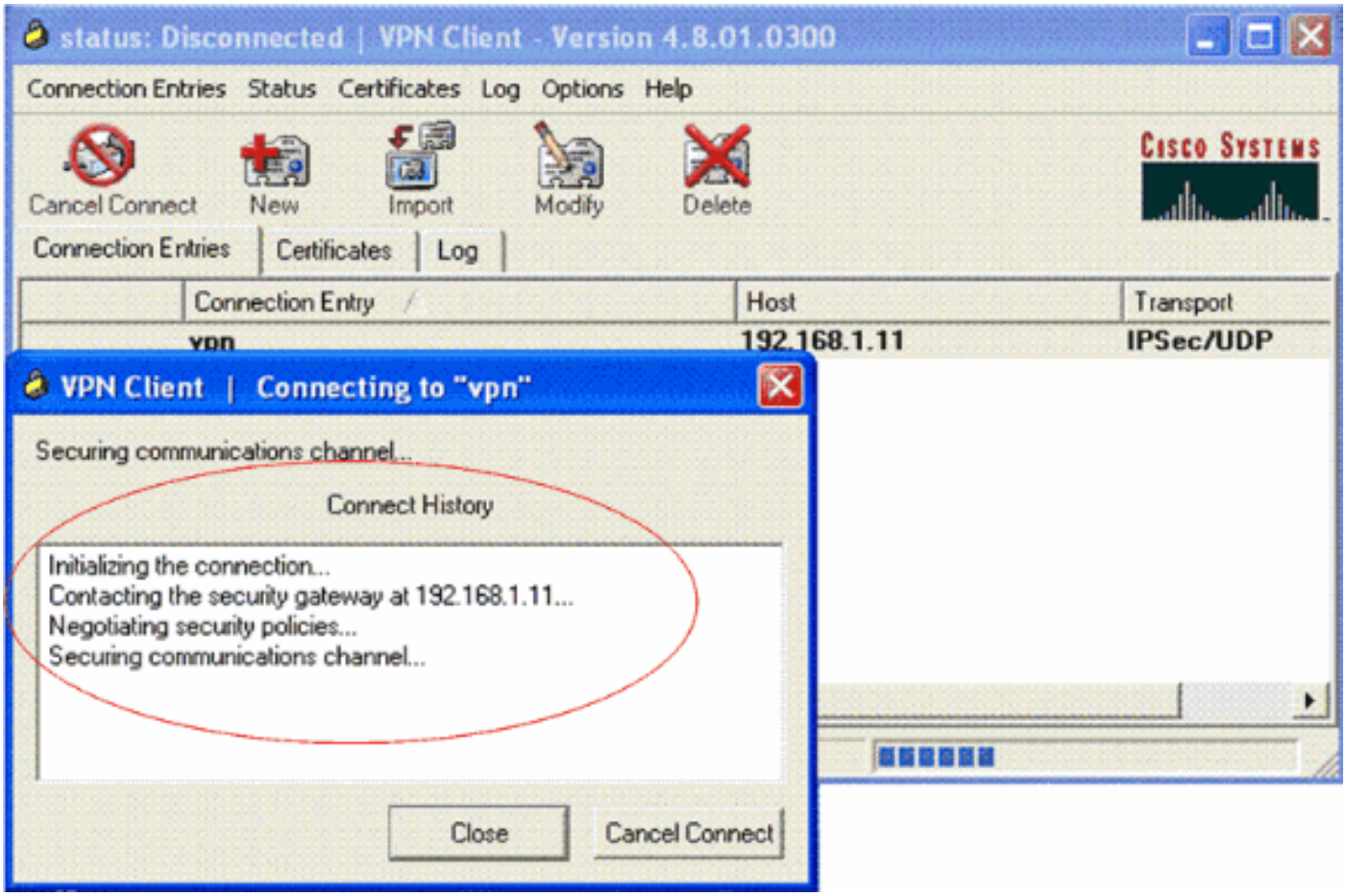
senha.

Verificar

A fim verificar esta configuração, configurar o SSID **vpnclient no** cliente Wireless com os mesmos parâmetros de segurança configurados no WLC e associe o cliente a este WLAN. Há diversos documentos que explicam como configurar um cliente Wireless com um perfil novo.

Uma vez que o cliente Wireless é associado, vá ao cliente VPN e clique sobre a conexão que você configurou. Clique então **conectam da** janela principal do cliente VPN.

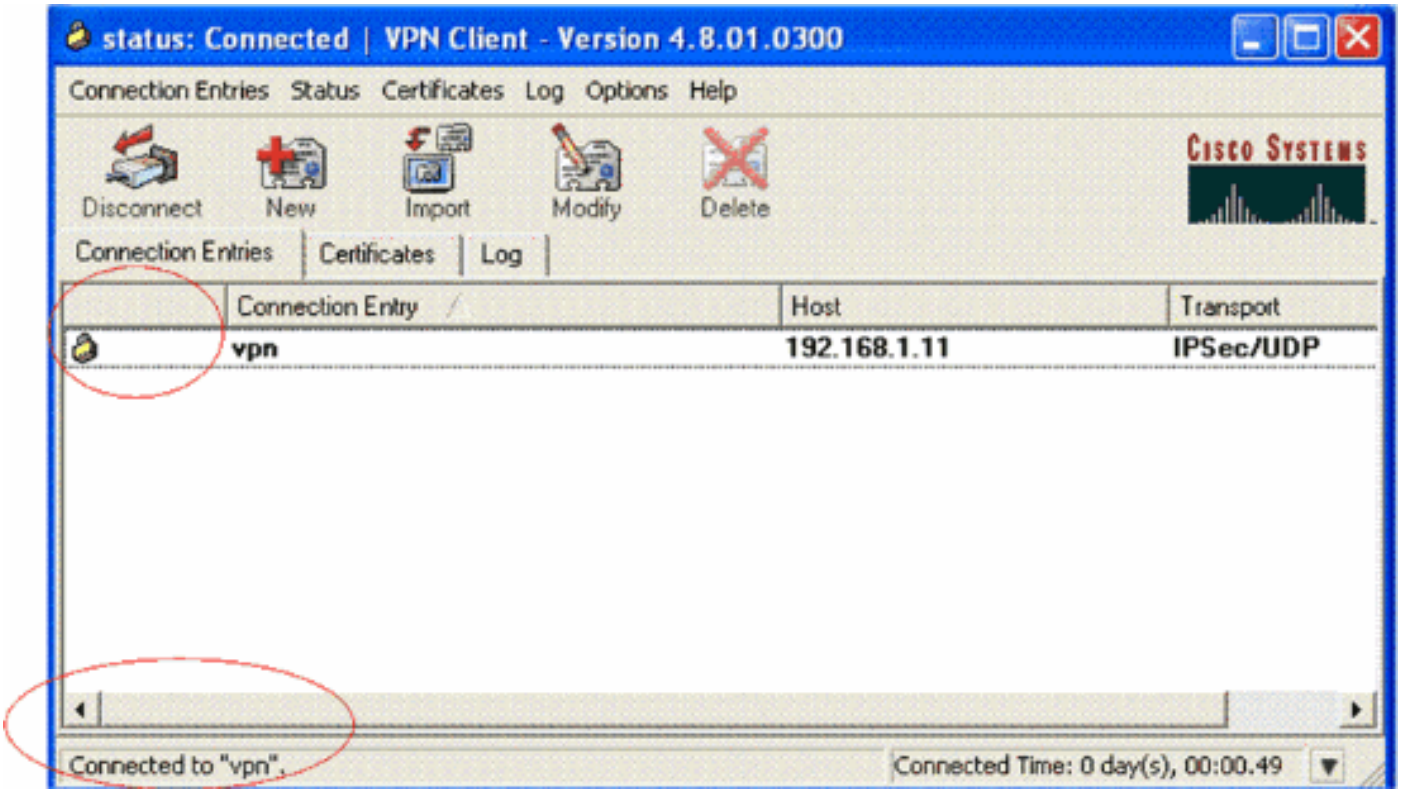
Você pode ver os parâmetros de segurança da fase 1 e da fase 2 negociados entre o cliente e o server.



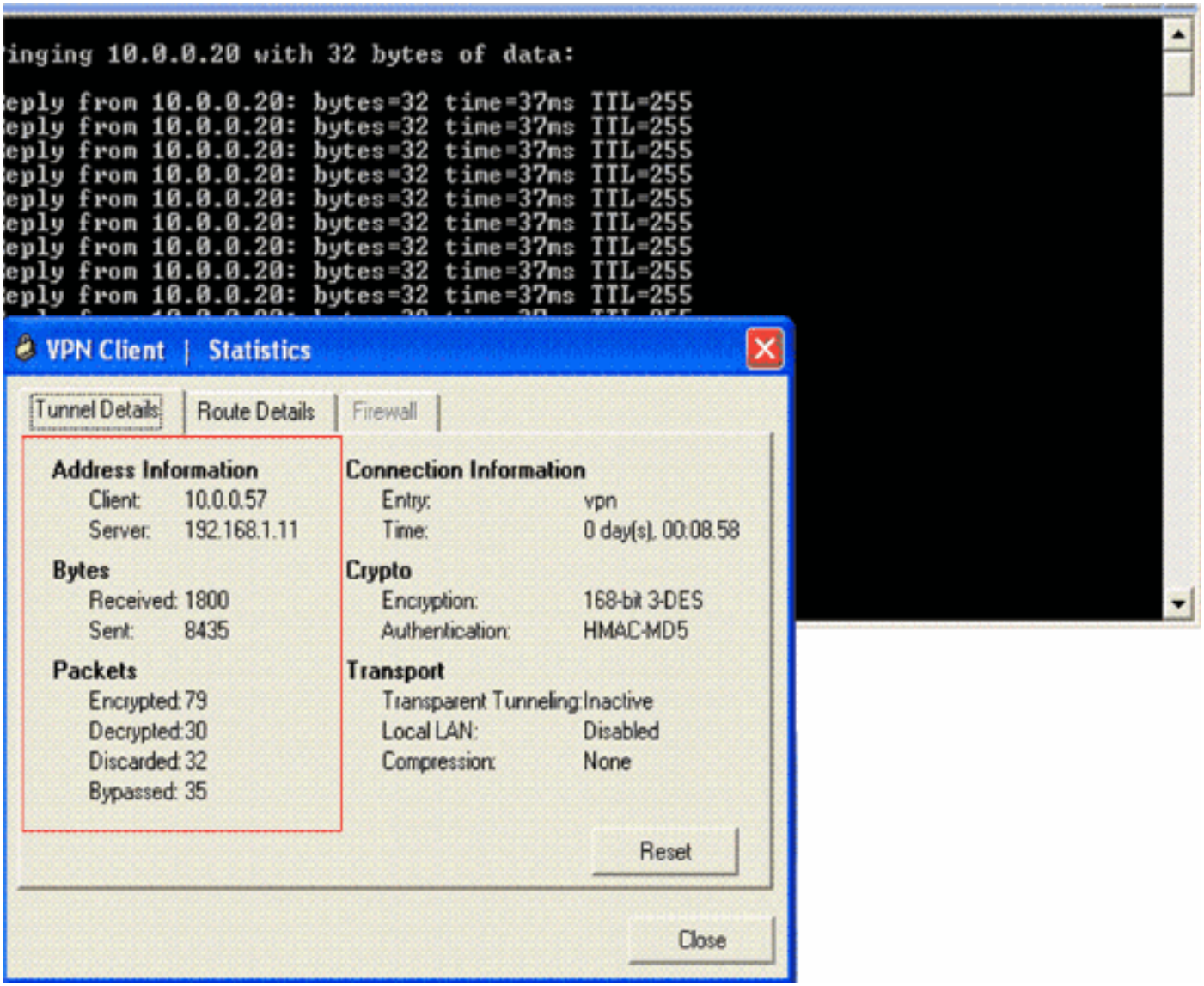
Nota: A fim estabelecer este túnel VPN, o cliente VPN e o server devem ter o IP reachability entre eles. Se o cliente VPN não pode contactar o gateway de segurança (servidor de VPN), a seguir o túnel não está estabelecido e uma caixa alerta é indicada no lado do cliente com esta mensagem:

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

A fim assegurar-se de que um túnel VPN esteja estabelecido corretamente entre o cliente e servidor, você pode encontrar um ícone do fechamento que seja criado ao lado do cliente VPN estabelecido. A barra de status igualmente indica **conectado ao "vpn"**. Exemplo:



Também, assegure-se de que você possa transmitir com sucesso e vice-versa dados ao segmento de LAN no lado de servidor do cliente VPN. Do menu principal do cliente VPN, escolha o **estado > as estatísticas**. Lá você pode encontrar as estatísticas dos pacotes criptografado e decriptografado que são passados através do túnel.



Neste tiro de tela, você pode ver o endereço de cliente como 10.0.0.57. Este é o endereço que o servidor de VPN atribui ao cliente de seu localmente conjunto configurado após a negociação bem sucedida da fase 1. O túnel é estabelecido uma vez, o servidor de VPN adiciona automaticamente uma rota a este endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído DHCP em sua tabela de rota.

Você pode igualmente ver o número de pacotes criptografado que aumentam quando os dados forem transferidos do cliente ao server e do número de pacotes decifrados que aumentam durante transferência de dados reversa.

Nota: Desde que o WLC é configurado para o VPN Passagem-através de, permite que o cliente alcance somente o segmento conectado com o gateway de VPN (aqui, é servidor de VPN de 192.168.1.11) configurado para Passagem-através de. Isto filtra todo tráfego restante.

Você pode verificar este configurando um outro servidor de VPN com a mesma configuração e configurar uma entrada da nova conexão para este servidor de VPN no cliente VPN. Agora, quando você tenta estabelecer um túnel com este servidor de VPN, não é bem sucedido. Isto é porque o WLC filtra este tráfego e permite um túnel somente ao endereço do gateway de VPN configurado para o VPN Passagem-através de.

Você pode igualmente verificar a configuração do CLI do servidor de VPN.

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**.

Estes **comandos show** usados no servidor de VPN puderam igualmente ser úteis ajudá-lo a verificar o status de túnel.

- O comando de **sessão de criptografia da mostra** é usado verificar o status de túnel. Estão aqui umas saídas de exemplo deste 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 cripto do isakmp da mostra** é usada para ver os parâmetros configurados da fase 1.

Troubleshooting

Os comandos debug and show explicados na seção da verificação podem igualmente ser usados para pesquisar defeitos.

- debug crypto isakmp
- debug crypto ipsec
- **mostre a sessão de criptografia**

- **O comando debug crypto isakmp no** servidor de VPN indica o processo de negociação inteiro da fase 1 entre o cliente e o server. Está aqui 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 de VPN indica a negociação de IPSec da fase 1 e a criação bem sucedidas 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
- Configurando a Segurança de rede IPSec
- Cisco Easy VPN Q&A
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- ACL no exemplo da configuração de controle do Wireless LAN
- Controlador do Wireless LAN (WLC) FAQ
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems