

ASA/PIX : ASDM と DHCP サーバを使用した IPsec VPN Client アドレス設定の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[リモート アクセス VPN \(IPsec \) の設定](#)

[CLI を使用した ASA/PIX の構成](#)

[Cisco VPN Client の設定](#)

[確認](#)

[show コマンド](#)

[トラブルシューティング](#)

[セキュリティ アソシエーションのクリア](#)

[トラブルシューティングのためのコマンド](#)

[デバッグの出力例](#)

[関連情報](#)

概要

このドキュメントでは、Adaptive Security Device Manager (ASDM) または CLI を使用して DHCP サーバがクライアント IP アドレスをすべての VPN Client に提供できるように Cisco 5500 シリーズ適応型セキュリティ アプライアンス (ASA) を設定する方法について説明します。ASDM では、直感的で使用が容易な Web ベースの管理インターフェイスにより、ワールドクラスのセキュリティ管理と監視機能が提供されています。Cisco ASA の設定が完了すると、Cisco VPN Client を使用して、これを確認できます。

Cisco VPN Client (4.x for Windows) と PIX 500 シリーズ セキュリティ アプライアンス 7.x との間にリモート アクセス VPN 接続を設定する方法については、「[PIX/ASA 7.x および Cisco VPN Client 4.x で Active Directory に対する Windows 2003 IAS RADIUS 認証を使用するための設定例](#)」を参照してください。リモートの VPN Client ユーザは Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS サーバを使用して Active Directory に対する認証を行います。

Cisco Secure Access Control Server (ACS バージョン 3.2) を使用して拡張認証 (Xauth) 用に、Cisco VPN Client (4.x for Windows) と PIX 500 シリーズ セキュリティ アプライアンス 7.x と

の間にリモート アクセス VPN 接続を設定する方法については、「[PIX/ASA 7.x と Cisco VPN Client 4.x の Cisco Secure ACS 認証用の設定例](#)」を参照してください。

前提条件

要件

このドキュメントでは、ASA が完全に動作していて、Cisco ASDM が CLI で設定を変更できるように設定されていることを想定しています。

注: 「[ASDM 用の HTTPS アクセスの許可](#)」または「[PIX/ASA 7.x: 内部および外部インターフェイスの SSH の設定例](#)」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Adaptive Security Device Manager バージョン 5.x 以降
- Cisco VPN Client バージョン 4.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

リモート アクセス VPN は、モバイル ユーザからの要求を処理し、組織のネットワークに安全に接続できるようにします。モバイル ユーザは、自身の PC にインストールした VPN Client ソフトウェアを使用して、安全な接続を確立できます。VPN Client は、これらの要求を受け入れるよう設定されている中央サイトのデバイスへの接続を開始します。この例で使用する中央サイトのデバイスは、ダイナミック暗号マップを使用する ASA 5500 シリーズの適応型セキュリティ アプライアンスです。

セキュリティ アプライアンスのアドレス管理では、トンネル経由でプライベート ネットワークのリソースにクライアントを接続する IP アドレスを設定する必要があります。そのようにして、クライアントがプライベート ネットワークに直接接続されているかのように機能するようにします。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベートネ

ットワークのアドレッシング方式で取得される IP アドレスを意味します。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 でのアドレスであり、ラボ環境で使用されたものです。

リモート アクセス VPN (IPsec) の設定

ASDM の手順

リモート アクセス VPN を設定するには、次の手順を実行します。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [IKE Policies] > [Add] の順に選択し、以下のように ISAKMP ポリシー 2 を作成します。
[OK]、[Apply] の順にクリックします。
2. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [IPSec Transform Sets] > [Add] の順に選択し、次のように **ESP-DES-SHA** トランスフォームを作成します。[OK]、[Apply] の順にクリックします。
3. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [Crypto Maps] > [Add] の順に選択し、次のような Priority 1 のダイナミック ポリシーを持つ暗号マップを作成します。[OK]、[Apply] の順にクリックします。
4. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [Group Policies] > [Add] > [Internal Group Policies] の順に選択し、以下のようにグループ ポリシー (例 : **GroupPloicy1**) を作成します。[OK]、[Apply] の順にクリックします。
5. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [Group Policies] > [Add] > [Internal Group Policies] > [Servers] の順に選択し、VPN Client ユーザの [DHCP Scope] が動的に割り当てられるように設定します。[OK]、[Apply] の順にクリックします。注: [DHCP Scope] の設定は任意です。詳細については、「[DHCP 機能のアドレッシング](#)」を参照してください。
6. [Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] の順に選択し、VPN Client アクセス用のユーザ アカウント (例 : Username - cisco123、Password - cisco123) を作成します。
7. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPSec Connection Profiles] > [Add] の順に選択し、次のようにトンネルグループ (たとえば、**TunnelGroup1** と事前共有鍵 cisco123) を追加します。[Basic] タブの [User Authentication] フィールドで、サーバグループとして [LOCAL] を選択します。[Default Group Policy] フィールドの [Group Policy] で [Grouppolicy1] を選択します。[DHCP Servers] 用のスペースに DHCP サ

ーバの IP アドレスを指定します。[OK] をクリックします。

8. [Advanced] > [Client Addressing] の順に選択し、DHCP サーバの [Use DHCP] チェックボックスをチェックし、IP アドレスを VPN Client に割り当てます。注: [Use authentication server] および [Use address pool] チェックボックスのチェックマークは外します。

ASDM 6.x の設定

ASDM のパスに関するマイナーな変更を除き、同じ ASDM 設定で ASDM バージョン 6.x は正常に機能します。特定のフィールドへの ASDM パスは、ASDM バージョン 6.2 以降と異なります。変更を既存のパスとともに以下に示します。ここで、ASDM のすべてのメジャーバージョンで変更がない場合は、グラフィック イメージは添付されません。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [IKE Policies] > [Add]
2. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [IPSec Transform Sets] > [Add]
3. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [Crypto Maps] > [Add]
4. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] > [Internal Group Policies] の順に選択します。
5. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] > [Internal Group Policies] > [Servers] の順に選択します。
6. [Configuration] > [Remote Access VPN] > [AAA Setup/Local Users] > [Local Users] > [Add] の順に選択します。
7. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPSec Connection Profiles] > [Add]
8. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] の順に選択します。次の 3 つのオプションは、デフォルトで有効になっています。Cisco ASA では、VPN Client にアドレスを割り当てるため、同じ順序に従います。その他の 2 つのオプションのチェックを外すと、Cisco ASA では AAA サーバとローカル プール オプションは確認されません。デフォルトで有効にされているオプションは、**show run all | in vpn-add** コマンドで確認できます。以下はサンプルの出力例です。
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 0 このコマンドの詳細については、「[vpn-addr-assign](#)」を参照してください。

CLI を使用した ASA/PIX の構成

後述のステップを実行して DHCP サーバを設定し、コマンドラインから VPN Client に IP アドレスを割り当てます。使用する各コマンドについての詳細は、『[リモートアクセス VPN の設定](#)』または『[Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、コマンドリファレンス](#)』を参照してください。

ASA デバイスでの設定の実行

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! -- Configure the outside and inside
```

```

interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 no failover icmp unreachable rate-limit 1 burst-
size 1 !--- Specify the location of the ASDM image for
ASA to fetch the image for ASDM access. asdm image
disk0:/asdm-613.bin no asdm history enable arp timeout
14400 global (outside) 1 192.168.1.5 nat (inside) 0
access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route
outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the DHCP Server and now by AAA or the Local
pool.The CLI vpn-addr-assign dhcp for VPN address
assignment through DHCP Server is hidden in the CLI
provided by show run command. no vpn-addr-assign aaa no
vpn-addr-assign local telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtcp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! group-policy GroupPolicy1 internal group-policy
GroupPolicy1 attributes !--- define the DHCP network
scope in the group policy.This configuration is Optional
dhcp-network-scope 192.168.5.0 !--- In order to identify
remote access users to the Security Appliance, !--- you
can also configure usernames and passwords on the
device. username cisco123 password ffIRPGpDSOJh9YLq
encrypted !--- Create a new tunnel group and set the
connection !--- type to remote-access. tunnel-group

```

```
TunnelGroup1 type remote-access !--- Define the DHCP
server address to the tunnel group. tunnel-group
TunnelGroup1 general-attributes default-group-policy
GroupPolicy1 dhcp-server 192.168.10.1 !--- Enter the
pre-shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

Cisco VPN Client の設定

ASA の設定に成功したことを確認するには、Cisco VPN Client を使用して Cisco ASA に接続してみます。

1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択します。
2. [New] をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。
3. 新しい接続の詳細情報を入力します。接続エントリの名前と説明を入力します。Host ボックスに、ASA の Outside の IP アドレスを入力します。次に、ASA で設定されている VPN トンネルグループ名 (TunnelGroup1) とパスワード (事前共有鍵 - cisco123) を入力します。[Save] をクリックします。
4. 使用する接続をクリックし、VPN クライアントのメイン ウィンドウにある [Connect] をクリックします。
5. プロンプトが表示されたら、Username : に cisco123、[Password:] に cisco123 と上記の ASA (Xauth) で設定されているように入力し、[OK] をクリックしてリモート ネットワークに接続します。
6. VPN Client が中央サイトの ASA に接続されます。
7. 接続が正常に確立されたら、[Status] メニューから [Statistics] を選択し、トンネルの詳細情報を確認します。

確認

show コマンド

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の show コマンドがサポートされています。OIT を使用して、show コマンド出力の解析を表示できます。

- show crypto isakmp sa : ピアの現在の IKE セキュリティ アソシエーション (SA) すべてを表示します。
- show crypto ipsec sa : 現在の SA が使用している設定を表示します。

```
ASA #show crypto ipsec sa interface: outside Crypto map tag: dynmap, seq num: 10, local addr:
192.168.1.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (192.168.5.1/255.255.255.0/0/0) current_peer: 192.168.1.2, username:
cisco123 dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 55, #pkts encrypt: 55, #pkts
digest: 55 #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag
successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0,
#decapsulated frgs needing reassembly: 0 #send errors:0, #recv errors: 0 local crypto endpt.:
192.168.1.1, remote crypto endpt.: 192.168.1.2 path mtu 1500, ipsec overhead 58, media mtu 1500
```

```
current outbound spi: C2C25E2B inbound esp sas: spi: 0x69F8C639 (1777911353) transform: esp-des
esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 40960, crypto-map: dynmap sa
timing: remaining key lifetime (sec): 28337 IV size: 8 bytes replay detection support: Y
outbound esp sas: spi: 0xC2C25E2B (3267517995) transform: esp-des esp-md5-hmac none in use
settings ={RA, Tunnel, } slot: 0, conn_id: 40960, crypto-map: dynmap sa timing: remaining key
lifetime (sec): 28337 IV size: 8 bytes replay detection support: Y ASA #show crypto isakmp sa
Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE
SA: 1 1 IKE Peer: 192.168.1.2 Type : user Role : responder Rekey : no State : AM_ACTIVE
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。デバッグ出力例も紹介しています。

注: リモートアクセス IPsec VPN の詳細は、『[一般的な L2L およびリモート アクセス IPsec VPN のトラブルシューティング方法について](#)』を参照してください。

セキュリティ アソシエーションのクリア

トラブルシューティングを行う際には、変更を加えた後、既存のセキュリティ アソシエーションを必ずクリアしてください。PIX の特権モードで、次のコマンドを使用します。

- `clear [crypto] ipsec sa` : アクティブな IPsec SA を削除します。crypto キーワードはオプションです。
- `clear [crypto] ipsec sa` : アクティブな IKE SA を削除します。crypto キーワードはオプションです。

トラブルシューティングのためのコマンド

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の `show` コマンドがサポートされています。OIT を使用して、`show` コマンド出力の解析を表示できます。

注: `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- `debug crypto ipsec 7` : フェーズ 2 の IPsec ネゴシエーションを表示します。
- `debug crypto isakmp 7` : フェーズ 1 の ISAKMP ネゴシエーションを表示します。

デバッグの出力例

- [ASA 8.0](#)
- [VPN Client 5.0 for Windows](#)

ASA 8.0

```
ASA#debug crypto isakmp 7 Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 856 Jan 22 22:21:24
[IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP =
192.168.1.2, processing ke payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing
ISA_KEY payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload Jan 22
22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]:
IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2,
Received xauth V6 VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
```

Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta tion capability flags: Main Mode: True Aggressive Mode: False Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V ID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group TunnelGroup1 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g IKE SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr oposal # 1, Transform # 13 acceptable Matches global IKE entry # 2 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ISAKMP SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ke payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing nonce payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin g keys for Responder... Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Cisco Unity VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing xauth V6 VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing dpd vid payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Fragmentation VID + extended capabilities payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti ga/Cisco VPN3000/Cisco ASA GW VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le ngth : 368 Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 116 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g notify payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408) Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received Cisco Unity client VID Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing blank hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing qm hash payload Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a 1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8 a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a ttr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin g MODE_CFG Reply attributes. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: IP Compression = disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, User (cisco123) authenticated. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143 60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE

RECEIVED Message (msgid=14 360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Processing cfg ACK attributes Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26 63aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Processing cfg Request attributes Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for IPV4 address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for IPV4 net mask! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for DNS server address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for WINS server address! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Received unsupported transaction mode attribute: 5 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Banner! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Save PW setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Default Domain Name! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Split Tunnel List! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Split DNS! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for PFS setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for backup ip-sec peer list! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Received unknown transaction mode attribute: 28684 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for Application Version! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Client Type: WinNT Client Application Version: 5.0.03.0530 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for FWTYPE! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12 3! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE_CFG: Received request for UDP Port! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth enabled) Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Assigned private IP address 192.168.5.1 to remote user Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Send Client Browser Proxy Attributes! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be included in the mode-cfg reply Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266 3aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, **PHASE 1 COMPLETED** Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection: DPD Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Starting P1 rekey timer: 950 seconds. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, sending notify message Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44 35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1022 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing

SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Received remote Proxy Host data in ID Payload: Address 192.168.5.1, Protocol 0, Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, QM IsRekeyed old sa not found by addr Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE Remote Peer configured for crypto map: dynmap Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing IPsec SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IPsec SA Proposal # 14, Transform # 1 acceptable Matches global IPSec SA entry # 10 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE: requesting SPI! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, oakley constructing quick mode Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing IPsec SA payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing IPsec nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing proxy ID Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Transmitting Proxy ID: Remote host: 192.168.5.1 Protocol 0 Port 0 Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Sending RESPONDER LIFETIME notification to Initiator Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 176 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=541f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, loading all IPSEC SAs Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Security negotiation complete for User (cisco123) Responder, Inbound SPI = 0x31de01d8, Outbound SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Starting P2 rekey timer: 27360 seconds. Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Adding static route for client address: 192.168.5.1 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, **PHASE 2 COMPLETED** (msgid=541f8e43) Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80 ASA#debug crypto ipsec 7 !--- Deletes the old SAs. ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 !--- Creates new SAs. ASA# IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI : 0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI

0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0 bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context 0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr: 192.168.5.1 Src mask: 255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: New inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: New inbound permit rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0

[VPN Client 5.0 for Windows](#)

VPN Client でログ レベルを有効にするには、[Log] > [Log settings] の順に選択します。

VPN Client でログ エントリを表示するには、[Log] > [Log Window] の順に選択します。

関連情報

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ](#)
- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、コマンドリファレンス](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス サポート ページ](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス、コマンドリファレンス](#)
- [Cisco Adaptive Security Device Manager](#)
- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [Cisco VPN Client に関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)