تكوين Cisco VPN مركز على TCP عبر IPSec مع عميل VPN الإصدارات 3.5 والإصدارات مع 3000 الأحدث

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين أمان IP (IPSec) عبر بروتوكول التحكم في الإرسال (TCP). هذا يمكن عميل VPN من العمل في بيئة لا يعمل فيها بروتوكول أمان التضمين القياسي (ESP، Protocol 50) أو تبادل مفتاح الإنترنت (IKE)، بروتوكول مخطط بيانات المستخدم (UDP) (500)، أو يمكن أن يعمل فقط مع تعديل قواعد جدار الحماية الموجودة. يقوم IPSec عبر TCP بتضمين كل من بروتوكولات IKE و IPSec داخل حزمة TCP، كما يعمل على تمكين الاتصال النفقي الآمن من خلال كل من أجهزة ترجمة عنوان الشبكة (NAT) وأجهزة ترجمة عنوان المنفذ (PAT) وجدران الحماية.

ملاحظة: لا يعمل IPSec عبر TCP مع جدران الحماية المستندة إلى الوكيل.

يعمل IPSec عبر TCP مع كل من عميل برنامج VPN وعميل الأجهزة VPN 3002. فهو عميل للتركيز فقط. لا يعمل لاتصالات LAN إلى LAN.

يمكن لتركيز VPN 3000 دعم بروتوكول IPSec القياسي وبروتوكول IPSec عبر TCP وبروتوكول IPSec عبر بروتوكول UDP في الوقت نفسه، وذلك استنادا إلى العميل الذي يتبادل البيانات معه.

يمكن لعميل أجهزة VPN 3002، الذي يدعم نفقا واحدا في كل مرة، الاتصال باستخدام IPSec القياسي أو IPSec عبر TCP أو IPSec عبر UDP.

المتطلبات الأساسية

المتطلبات

يجب تكوين الواجهة العامة لتركيز VPN 3000. يتم دعم IPSec عبر TCP فقط على الواجهة العامة على إيثرنت 2. راجع ملاحظات إصدار عميل Cisco VPN للحصول على مزيد من المعلومات.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- VPN 3000 Concentrator الإصدار 3.5 أو إصدار أحدث
- VPN Client الإصدار 3.5 أو إصدار أحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

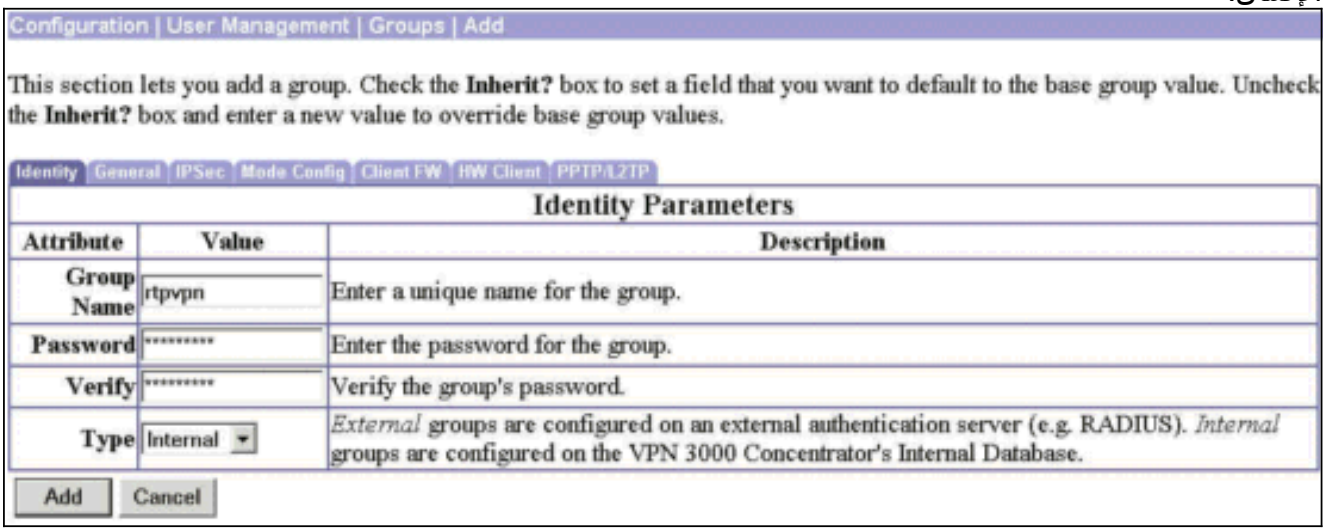
للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

تكوين مركز VPN 3000

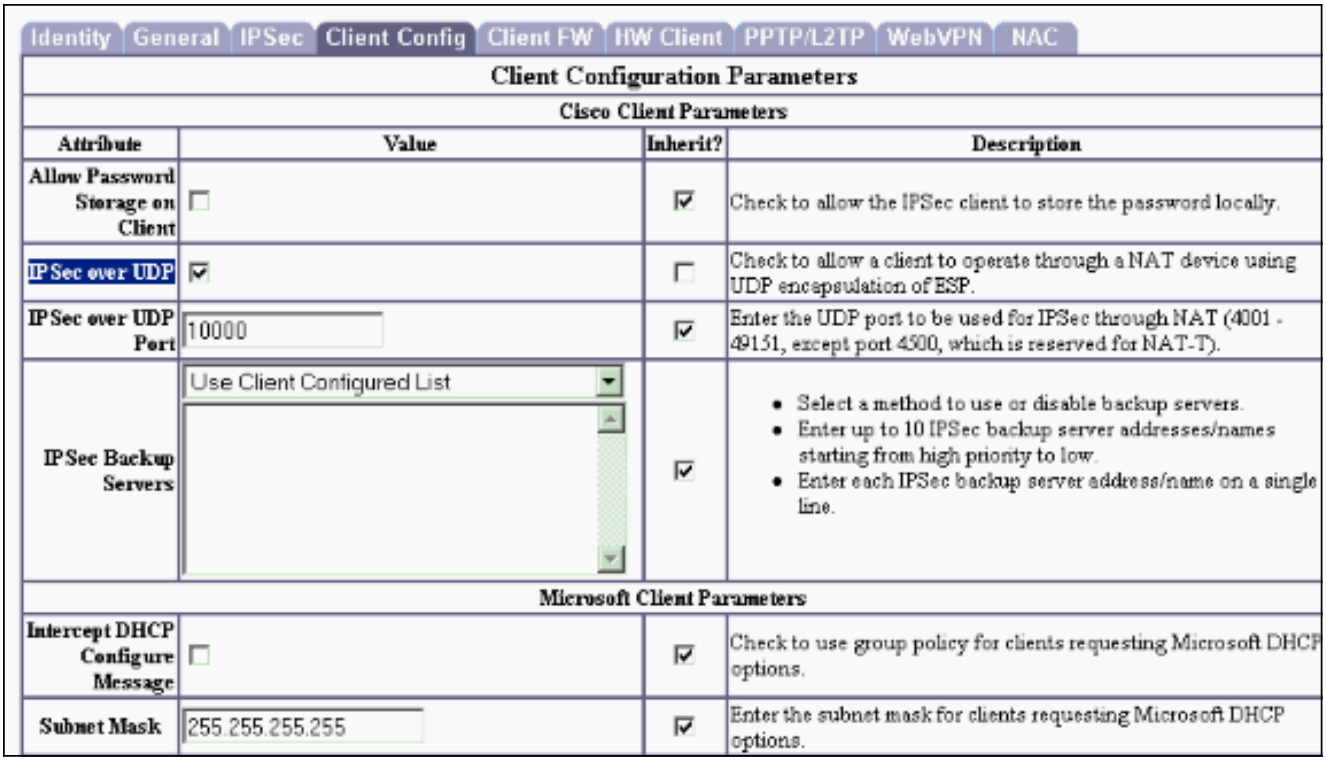
التعليمات بالتفصيل

أكمل هذه الخطوات لتكوين مركز VPN 3000.

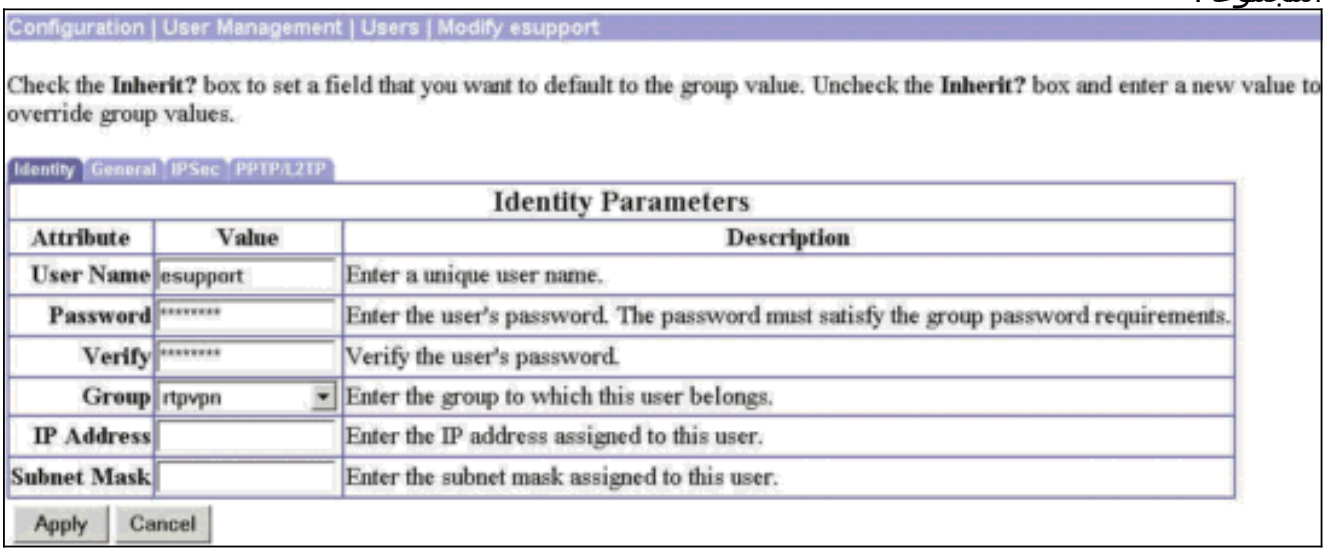
1. انتقل إلى **التكوين>إدارة المستخدم>المجموعات>إضافة مجموعة** وإنشاء اسم مجموعة وكلمة مرور على مركز VPN. طقطقة **يضيف** عند الإكمال.



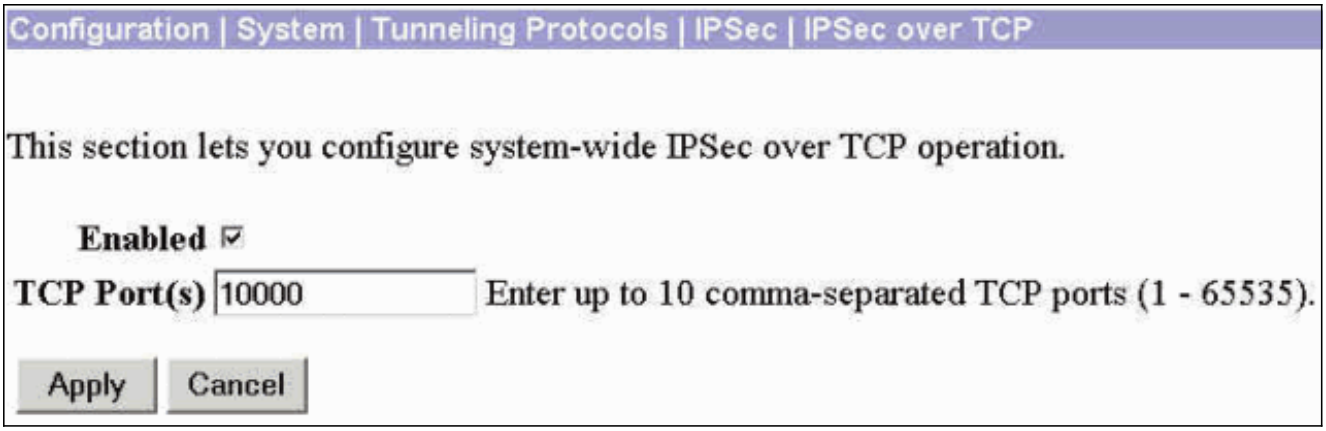
2. إذا كان نفس المجموعة قيد الاستخدام من قبل المستخدمين في إصدارات عميل VPN الأقدم من 3.5، أو إذا كنت تستخدم IPSec عبر UDP على عميل VPN، فحدد **IPSec عبر UDP** ضمن علامة التبويب تكوين العميل.



3. انتقل إلى **التكوين>إدارة المستخدم>المستخدمين>تعديل الدعم**. إذا كنت تستخدم مصادقة داخلية، فقم بإنشاء مستخدم للمصادقة على المجموعة. ثم قم بتعيين المستخدم لهذه المجموعة.



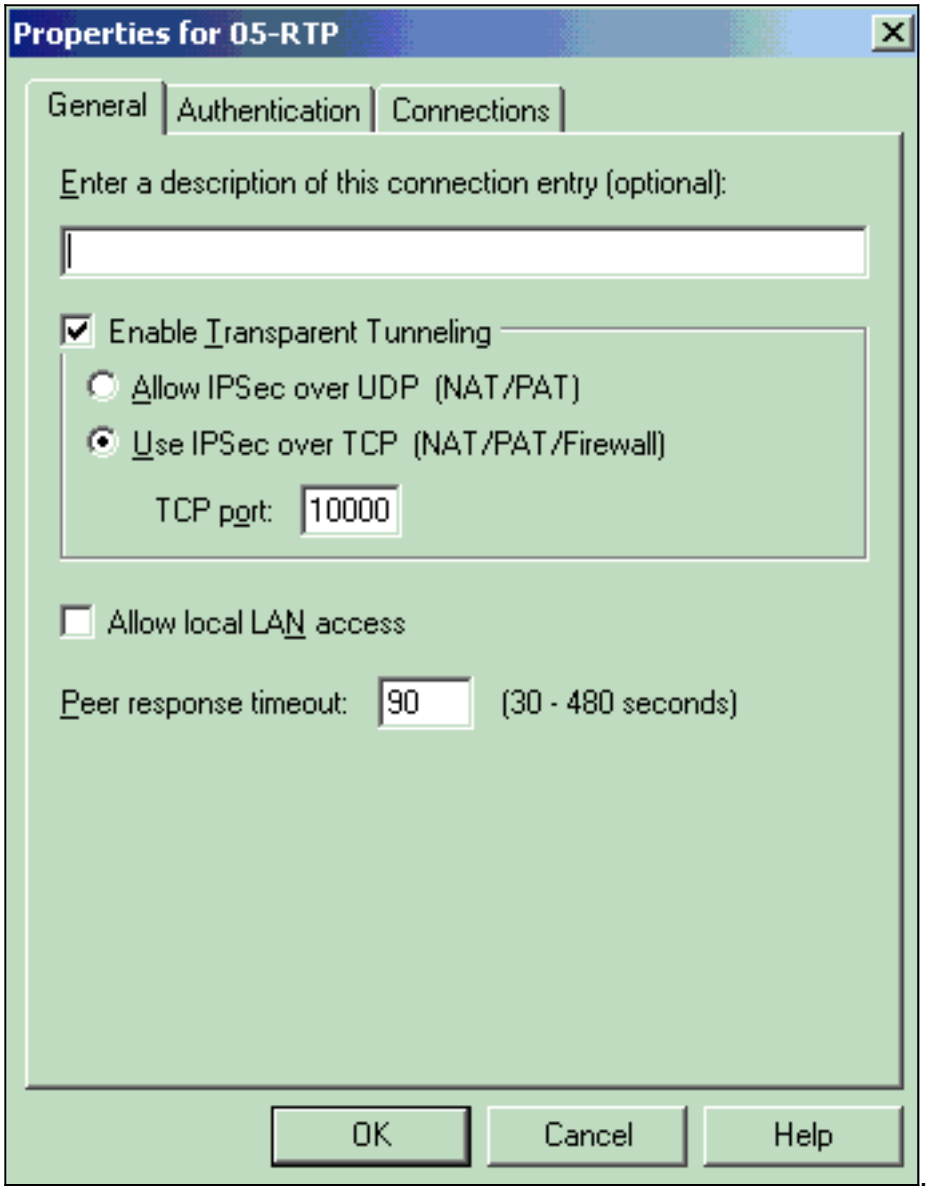
4. انتقل إلى **التكوين > الاتصال النفقي والأمان > شفافية NAT** وحدد خيار **IPsec عبر TCP**أدخل ما يصل إلى 10 منافذ، باستخدام فاصلة لفصل المنافذ. لا تحتاج لاستخدام مسافات. المنفذ الافتراضي هو 10000. المدى هو من 1 إلى 65،635.إذا قمت بإدخال منفذ معروف (مثل المنفذ 80 (HTTP) أو المنفذ 443 (HTTPS)، يعرض النظام تحذيرا بأن البروتوكول المرتبط بذلك المنفذ لم يعد يعمل على الواجهة العامة. والنتيجة هي أنه لم يعد بإمكانك إستخدام مستعرض لإدارة مركز VPN 3000 من خلال الواجهة العامة. لحل هذه المشكلة، قم بإعادة تكوين إدارة HTTP/HTTPS إلى منافذ مختلفة.يجب تكوين منفذ (منافذ) TCP على عميل شبكة VPN وكذلك على مركز شبكة VPN. يجب أن يتضمن تكوين العميل منفذا واحدا على الأقل من المنافذ التي قمت بتعيينها لمركز تركيز الشبكة الخاصة الظاهرية (VPN) هنا.



تكوين عميل VPN

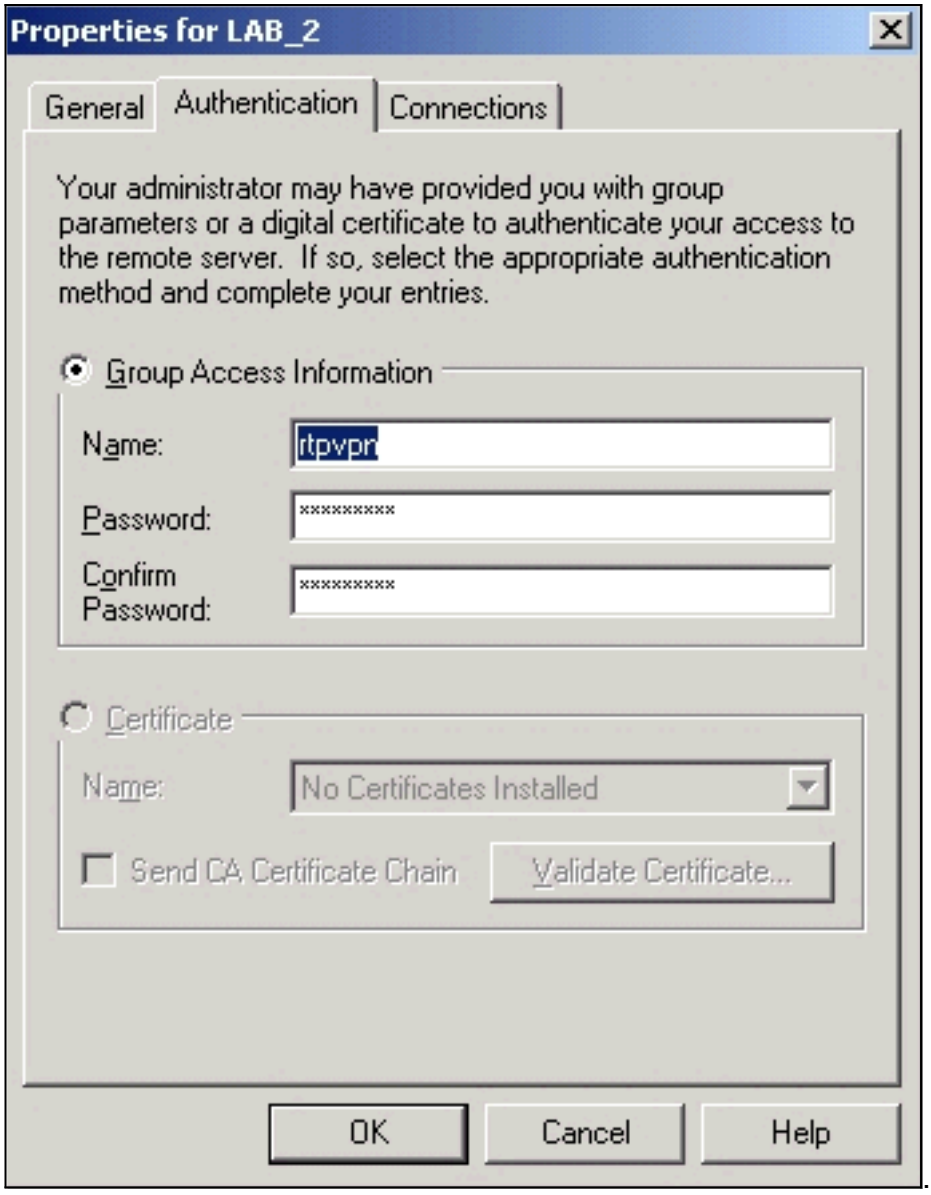
أكمل هذه الخطوات لتكوين عميل شبكة VPN.

1. انتقل إلى **الخيارات** > **الخصائص**. تحت علامة التبويب "عام"، تحقق من **تمكين الاتصال النفقي الشفاف** واختر **إستخدام IPSec عبر TCP**



((NAT/PAT/Firewall.

2. تحت علامة التبويب مصادقة، قم بتكوين اسم مجموعة وكلمة مرور على



العميل.

التحقق من الاتصالات على مركز VPN 3000

يتحقق **ال monitore>جلسة** منطقة على ال VPN 3000 مركز من توصيل المستخدمين مع نفس المجموعة ل IPSec عبر TCP و IPSec عبر UDP.

Monitoring | Sessions — Wednesday, 05 December 2001 10:39:0

Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group --All--

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	2	1	3	3	20	26

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
esupport	rtpvpn	64.102.55.209	172.18.124.217	IPSec/UDP	3DES-168	Dec 05 10:38:06	0:00:58	22416	1536
esupporttcp	rtpvpn	172.18.124.241	172.18.124.218	IPSec/TCP	3DES-168	Dec 05 10:39:02	0:00:02	64	72

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

قم بتمكين تصحيح الأخطاء ل AUTH و AUTHDBG و AUTHDECODE و IKE و IKEDBG و IKEdecode و IPSec و IPSECDBG و IPSECDECODE للمستويات من 1 إلى 13 تحت **التكوين > النظام > الأحداث > الفئات**.

```
SEV=9 IKEDBG/0 RPT=5347 172.18.124.241 11:40:54.220 12/05/2001 1203
                                    [Group [rtpvpn] User [esupporttcp
                                        processing SA payload

SEV=8 IKEDECODE/0 RPT=5035 172.18.124.241 11:40:54.220 12/05/2001 1204
                                        : SA Payload Decode
                                            (DOI : IPSEC (1
                                    (Situation : Identity Only (1
                                            Length : 696

SEV=8 IKEDECODE/0 RPT=5036 172.18.124.241 11:40:54.220 12/05/2001 1207
                                          :Proposal Decode
                                            Proposal # : 1
                                    (Protocol ID : ESP (3
                                        of Transforms: 1#
                                        Spi : 98 79 D2 38
                                            Length : 40

SEV=8 IKEDECODE/0 RPT=5037 172.18.124.241 11:40:54.220 12/05/2001 1211
                                    :Transform # 1 Decode for Proposal # 1
```

Transform # : 1
(Transform ID : Triple-DES (3
Length : 28

SEV=8 IKEDECODE/0 RPT=5038 172.18.124.241 11:40:54.220 12/05/2001 1213
:Phase 2 SA Attribute Decode for Transform # 1
(HMAC Algorithm: MD5 (1
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5039 172.18.124.241 11:40:54.220 12/05/2001 1216
:Proposal Decode
Proposal # : 1
(Protocol ID : IPCOMP (4
of Transforms: 1#
Spi : 5D 82
Length : 34

SEV=8 IKEDECODE/0 RPT=5040 172.18.124.241 11:40:54.220 12/05/2001 1220
:Transform # 1 Decode for Proposal # 1
Transform # : 1
(Transform ID : LZS (3
Length : 24

SEV=8 IKEDECODE/0 RPT=5041 172.18.124.241 11:40:54.220 12/05/2001 1222
:Phase 2 SA Attribute Decode for Transform # 1
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5042 172.18.124.241 11:40:54.220 12/05/2001 1224
:Proposal Decode
Proposal # : 2
(Protocol ID : ESP (3
of Transforms: 1#
Spi : 98 79 D2 38
Length : 40

SEV=8 IKEDECODE/0 RPT=5043 172.18.124.241 11:40:54.220 12/05/2001 1228
:Transform # 1 Decode for Proposal # 2
Transform # : 1
(Transform ID : Triple-DES (3
Length : 28

SEV=8 IKEDECODE/0 RPT=5044 172.18.124.241 11:40:54.220 12/05/2001 1230
:Phase 2 SA Attribute Decode for Transform # 1
(HMAC Algorithm: SHA (2
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5045 172.18.124.241 11:40:54.220 12/05/2001 1233
:Proposal Decode
Proposal # : 2
(Protocol ID : IPCOMP (4
of Transforms: 1#
Spi : D8 44
Length : 34

SEV=8 IKEDECODE/0 RPT=5046 172.18.124.241 11:40:54.220 12/05/2001 1237
:Transform # 1 Decode for Proposal # 2
Transform # : 1
(Transform ID : LZS (3
Length : 24

SEV=8 IKEDECODE/0 RPT=5047 172.18.124.241 11:40:54.220 12/05/2001 1239

:Phase 2 SA Attribute Decode for Transform # 1
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5048 172.18.124.241 11:40:54.220 12/05/2001 1241
:Proposal Decode
Proposal # : 3
(Protocol ID : ESP (3
of Transforms: 1#
Spi : 98 79 D2 38
Length : 40

SEV=8 IKEDECODE/0 RPT=5049 172.18.124.241 11:40:54.220 12/05/2001 1245
:Transform # 1 Decode for Proposal # 3
Transform # : 1
(Transform ID : Triple-DES (3
Length : 28

SEV=8 IKEDECODE/0 RPT=5050 172.18.124.241 11:40:54.220 12/05/2001 1247
:Phase 2 SA Attribute Decode for Transform # 1
(HMAC Algorithm: MD5 (1
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5051 172.18.124.241 11:40:54.220 12/05/2001 1250
:Proposal Decode
Proposal # : 4
(Protocol ID : ESP (3
of Transforms: 1#
Spi : 98 79 D2 38
Length : 40

SEV=8 IKEDECODE/0 RPT=5052 172.18.124.241 11:40:54.220 12/05/2001 1254
:Transform # 1 Decode for Proposal # 4
Transform # : 1
(Transform ID : Triple-DES (3
Length : 28

SEV=8 IKEDECODE/0 RPT=5053 172.18.124.241 11:40:54.220 12/05/2001 1256
:Phase 2 SA Attribute Decode for Transform # 1
(HMAC Algorithm: SHA (2
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5054 172.18.124.241 11:40:54.220 12/05/2001 1259
:Proposal Decode
Proposal # : 5
(Protocol ID : ESP (3
of Transforms: 1#
Spi : 98 79 D2 38
Length : 40

SEV=8 IKEDECODE/0 RPT=5055 172.18.124.241 11:40:54.220 12/05/2001 1263
:Transform # 1 Decode for Proposal # 5
Transform # : 1
(Transform ID : DES-CBC (2
Length : 28

SEV=8 IKEDECODE/0 RPT=5056 172.18.124.241 11:40:54.220 12/05/2001 1265
:Phase 2 SA Attribute Decode for Transform # 1
(HMAC Algorithm: MD5 (1
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

```
SEV=8 IKEDECODE/0 RPT=5057 172.18.124.241 11:40:54.220 12/05/2001 1268
                                                        :Proposal Decode
                                                          Proposal # : 5
                                                 (Protocol ID : IPCOMP (4
                                                        of Transforms: 1#
                                                             Spi : 80 07
                                                             Length : 34

SEV=8 IKEDECODE/0 RPT=5058 172.18.124.241 11:40:54.220 12/05/2001 1272
                                     :Transform # 1 Decode for Proposal # 5
                                                           Transform # : 1
                                               (Transform ID : LZS (3
                                                             Length : 24

SEV=8 IKEDECODE/0 RPT=5059 172.18.124.241 11:40:54.220 12/05/2001 1274
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                 (Encapsulation : Tunnel (1
                                              Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5060 172.18.124.241 11:40:54.220 12/05/2001 1276
                                                        :Proposal Decode
                                                          Proposal # : 6
                                                  (Protocol ID : ESP (3
                                                      of Transforms: 1#
                                                      Spi : 98 79 D2 38
                                                             Length : 40

SEV=8 IKEDECODE/0 RPT=5061 172.18.124.241 11:40:54.220 12/05/2001 1280
                                     :Transform # 1 Decode for Proposal # 6
                                                           Transform # : 1
                                               (Transform ID : DES-CBC (2
                                                             Length : 28

SEV=8 IKEDECODE/0 RPT=5062 172.18.124.241 11:40:54.220 12/05/2001 1282
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                (HMAC Algorithm: SHA (2
                                                 (Encapsulation : Tunnel (1
                                              Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5063 172.18.124.241 11:40:54.220 12/05/2001 1285
                                                        :Proposal Decode
                                                          Proposal # : 6
                                                 (Protocol ID : IPCOMP (4
                                                        of Transforms: 1#
                                                             Spi : 1A D4
                                                             Length : 34

SEV=8 IKEDECODE/0 RPT=5064 172.18.124.241 11:40:54.220 12/05/2001 1289
                                     :Transform # 1 Decode for Proposal # 6
                                                           Transform # : 1
                                               (Transform ID : LZS (3
                                                             Length : 24

SEV=8 IKEDECODE/0 RPT=5065 172.18.124.241 11:40:54.220 12/05/2001 1291
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                 (Encapsulation : Tunnel (1
                                              Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5066 172.18.124.241 11:40:54.220 12/05/2001 1293
                                                        :Proposal Decode
                                                          Proposal # : 7
                                                  (Protocol ID : ESP (3
                                                      of Transforms: 1#
                                                      Spi : 98 79 D2 38
```

```
                                                                Length : 40

SEV=8 IKEDECODE/0 RPT=5067 172.18.124.241 11:40:54.220 12/05/2001 1297
                                    :Transform # 1 Decode for Proposal # 7
                                                          Transform # : 1
                                                 (Transform ID : DES-CBC (2
                                                              Length : 28

SEV=8 IKEDECODE/0 RPT=5068 172.18.124.241 11:40:54.220 12/05/2001 1299
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                    (HMAC Algorithm: MD5 (1
                                                 (Encapsulation : Tunnel (1
                                                Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5069 172.18.124.241 11:40:54.220 12/05/2001 1302
                                                           :Proposal Decode
                                                             Proposal # : 8
                                                  (Protocol ID : ESP (3
                                                      of Transforms: 1#
                                                      Spi : 98 79 D2 38
                                                              Length : 40

SEV=8 IKEDECODE/0 RPT=5070 172.18.124.241 11:40:54.220 12/05/2001 1306
                                    :Transform # 1 Decode for Proposal # 8
                                                          Transform # : 1
                                                 (Transform ID : DES-CBC (2
                                                              Length : 28

SEV=8 IKEDECODE/0 RPT=5071 172.18.124.241 11:40:54.220 12/05/2001 1308
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                    (HMAC Algorithm: SHA (2
                                                 (Encapsulation : Tunnel (1
                                                Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5072 172.18.124.241 11:40:54.220 12/05/2001 1311
                                                           :Proposal Decode
                                                             Proposal # : 9
                                                  (Protocol ID : ESP (3
                                                      of Transforms: 1#
                                                      Spi : 98 79 D2 38
                                                              Length : 40

SEV=8 IKEDECODE/0 RPT=5073 172.18.124.241 11:40:54.220 12/05/2001 1315
                                    :Transform # 1 Decode for Proposal # 9
                                                          Transform # : 1
                                                (Transform ID : NULL (11
                                                              Length : 28

SEV=8 IKEDECODE/0 RPT=5074 172.18.124.241 11:40:54.220 12/05/2001 1317
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                    (HMAC Algorithm: MD5 (1
                                                 (Encapsulation : Tunnel (1
                                                Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5075 172.18.124.241 11:40:54.220 12/05/2001 1320
                                                           :Proposal Decode
                                                             Proposal # : 9
                                                (Protocol ID : IPCOMP (4
                                                      of Transforms: 1#
                                                           Spi : 7B 9B
                                                              Length : 34

SEV=8 IKEDECODE/0 RPT=5076 172.18.124.241 11:40:54.230 12/05/2001 1324
                                    :Transform # 1 Decode for Proposal # 9
```

```
                                                    Transform # : 1
                                                (Transform ID : LZS (3
                                                    Length : 24

SEV=8 IKEDECODE/0 RPT=5077 172.18.124.241 11:40:54.230 12/05/2001 1326
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                (Encapsulation : Tunnel (1
                                               Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5078 172.18.124.241 11:40:54.230 12/05/2001 1328
                                                    :Proposal Decode
                                                    Proposal # : 10
                                                (Protocol ID : ESP (3
                                                    of Transforms: 1#
                                                    Spi : 98 79 D2 38
                                                    Length : 40

SEV=8 IKEDECODE/0 RPT=5079 172.18.124.241 11:40:54.230 12/05/2001 1332
                                    :Transform # 1 Decode for Proposal # 10
                                                    Transform # : 1
                                                (Transform ID : NULL (11
                                                    Length : 28

SEV=8 IKEDECODE/0 RPT=5080 172.18.124.241 11:40:54.230 12/05/2001 1334
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                (HMAC Algorithm: SHA (2
                                                (Encapsulation : Tunnel (1
                                               Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5081 172.18.124.241 11:40:54.230 12/05/2001 1337
                                                    :Proposal Decode
                                                    Proposal # : 10
                                                (Protocol ID : IPCOMP (4
                                                    of Transforms: 1#
                                                    Spi : 79 45
                                                    Length : 34

SEV=8 IKEDECODE/0 RPT=5082 172.18.124.241 11:40:54.230 12/05/2001 1341
                                    :Transform # 1 Decode for Proposal # 10
                                                    Transform # : 1
                                                (Transform ID : LZS (3
                                                    Length : 24

SEV=8 IKEDECODE/0 RPT=5083 172.18.124.241 11:40:54.230 12/05/2001 1343
                            :Phase 2 SA Attribute Decode for Transform # 1
                                                (Encapsulation : Tunnel (1
                                               Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5084 172.18.124.241 11:40:54.230 12/05/2001 1345
                                                    :Proposal Decode
                                                    Proposal # : 11
                                                (Protocol ID : ESP (3
                                                    of Transforms: 1#
                                                    Spi : 98 79 D2 38
                                                    Length : 40

SEV=8 IKEDECODE/0 RPT=5085 172.18.124.241 11:40:54.230 12/05/2001 1349
                                    :Transform # 1 Decode for Proposal # 11
                                                    Transform # : 1
                                                (Transform ID : NULL (11
                                                    Length : 28

SEV=8 IKEDECODE/0 RPT=5086 172.18.124.241 11:40:54.230 12/05/2001 1351
                            :Phase 2 SA Attribute Decode for Transform # 1
```

(HMAC Algorithm: MD5 (1
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=8 IKEDECODE/0 RPT=5087 172.18.124.241 11:40:54.230 12/05/2001 1354
:Proposal Decode
Proposal # : 12
(Protocol ID : ESP (3
of Transforms: 1#
Spi : 98 79 D2 38
Length : 40

SEV=8 IKEDECODE/0 RPT=5088 172.18.124.241 11:40:54.230 12/05/2001 1358
:Transform # 1 Decode for Proposal # 12
Transform # : 1
(Transform ID : NULL (11
Length : 28

SEV=8 IKEDECODE/0 RPT=5089 172.18.124.241 11:40:54.230 12/05/2001 1360
:Phase 2 SA Attribute Decode for Transform # 1
(HMAC Algorithm: SHA (2
(Encapsulation : Tunnel (1
Life Time : 2147483 seconds

SEV=9 IKEDBG/1 RPT=666 172.18.124.241 11:40:54.230 12/05/2001 1363
[Group [rtpvpn] User [esupporttcp
processing nonce payload

SEV=9 IKEDBG/1 RPT=667 172.18.124.241 11:40:54.230 12/05/2001 1364
[Group [rtpvpn] User [esupporttcp
Processing ID

SEV=12 IKEDECODE/11 RPT=115 11:40:54.230 12/05/2001 1365
ID_IPV4_ADDR ID received
172.18.124.217

SEV=5 IKE/25 RPT=58 172.18.124.241 11:40:54.230 12/05/2001 1366
[Group [rtpvpn] User [esupporttcp
:Received remote Proxy Host data in ID Payload
Address 172.18.124.217, Protocol 0, Port 0

SEV=9 IKEDBG/1 RPT=668 172.18.124.241 11:40:54.230 12/05/2001 1369
[Group [rtpvpn] User [esupporttcp
Processing ID

SEV=12 IKEDECODE/11 RPT=116 11:40:54.230 12/05/2001 1370
ID_IPV4_ADDR_SUBNET ID received
0.0.0.0
0.0.0.0

SEV=5 IKE/34 RPT=36 172.18.124.241 11:40:54.230 12/05/2001 1371
[Group [rtpvpn] User [esupporttcp
:Received local IP Proxy Subnet data in ID Payload
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

SEV=5 IKE/66 RPT=58 172.18.124.241 11:40:54.230 12/05/2001 1374
[Group [rtpvpn] User [esupporttcp
IKE Remote Peer configured for SA: ESP-3DES-MD5

SEV=9 IKEDBG/0 RPT=5348 172.18.124.241 11:40:54.230 12/05/2001 1376
[Group [rtpvpn] User [esupporttcp
processing IPSEC SA

SEV=12 IKEDECODE/0 RPT=5090 11:40:54.230 12/05/2001 1377

```
                                :IKE Decode of received SA attributes follows
              ..... 00020004 80010001 80040001 80050001 :0000
                                                .. . 0020C49B :0010

                  SEV=12 IKEDECODE/0 RPT=5091 11:40:54.230 12/05/2001 1380
                                :IKE Decode of received SA attributes follows
              ..... 00020004 80010001 80040001 80050002 :0000
                                                .. . 0020C49B :0010

                       SEV=8 IKEDBG/0 RPT=5349 11:40:54.230 12/05/2001 1383
                       Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
                                          :Parsing received transform
                                                       :Phase 2 failure
                            :Mismatched attr types for class HMAC Algorithm
                                                              Rcv'd: SHA
                                                              Cfg'd: MD5

                  SEV=12 IKEDECODE/0 RPT=5092 11:40:54.230 12/05/2001 1387
                                :IKE Decode of received SA attributes follows
              ..... 00020004 80010001 80040001 80050001 :0000
                                                .. . 0020C49B :0010

          SEV=7 IKEDBG/27 RPT=58 172.18.124.241 11:40:54.230 12/05/2001 1390
                                          [Group [rtpvpn] User [esupporttcp
                        IPSec SA Proposal # 3, Transform # 1 acceptable

        SEV=7 IKEDBG/0 RPT=5350 172.18.124.241 11:40:54.230 12/05/2001 1392
                                          [Group [rtpvpn] User [esupporttcp
                                                    !IKE: requesting SPI

                     SEV=9 IPSECDBG/6 RPT=282 11:40:54.230 12/05/2001 1393
,IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000
                ,seq 58, err 0, type 2, mode 0, state 32, label 0, pad 0
              ,spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0
          hmacAlg 0, lifetype 0, lifetime1 707832, lifetime2 0, dsId 300

                   SEV=9 IPSECDBG/1 RPT=1062 11:40:54.230 12/05/2001 1397
                                          !Processing KEY_GETSPI msg

                   SEV=7 IPSECDBG/13 RPT=58 11:40:54.230 12/05/2001 1398
                                             Reserved SPI 1889854019

                      SEV=8 IKEDBG/6 RPT=58 11:40:54.230 12/05/2001 1399
                           IKE got SPI from key engine: SPI = 0x70a4e243

        SEV=9 IKEDBG/0 RPT=5351 172.18.124.241 11:40:54.230 12/05/2001 1400
                                          [Group [rtpvpn] User [esupporttcp
                                              oakley constucting quick mode

        SEV=9 IKEDBG/0 RPT=5352 172.18.124.241 11:40:54.230 12/05/2001 1401
                                          [Group [rtpvpn] User [esupporttcp
                                                    constructing blank hash

        SEV=9 IKEDBG/0 RPT=5353 172.18.124.241 11:40:54.230 12/05/2001 1402
                                          [Group [rtpvpn] User [esupporttcp
                                              constructing ISA_SA for ipsec

         SEV=9 IKEDBG/1 RPT=669 172.18.124.241 11:40:54.230 12/05/2001 1403
                                          [Group [rtpvpn] User [esupporttcp
                                           constructing ipsec nonce payload

         SEV=9 IKEDBG/1 RPT=670 172.18.124.241 11:40:54.230 12/05/2001 1404
                                          [Group [rtpvpn] User [esupporttcp
                                                      constructing proxy ID
```

```
SEV=7 IKEDBG/0 RPT=5354 172.18.124.241 11:40:54.230 12/05/2001 1405
                                    [Group [rtpvpn] User [esupporttcp
                                              :Transmitting Proxy Id
                          Remote host: 172.18.124.217 Protocol 0 Port 0
                  Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

SEV=9 IKEDBG/0 RPT=5355 172.18.124.241 11:40:54.230 12/05/2001 1409
                                    [Group [rtpvpn] User [esupporttcp
                                          constructing qm hash

             SEV=12 IKEDECODE/5 RPT=58 11:40:54.240 12/05/2001 1410
                IKE Responder sending 2nd QM pkt: msg id = f2a6ce35

SEV=8 IKEDBG/0 RPT=5356 172.18.124.241 11:40:54.240 12/05/2001 1411
                     : SENDING Message (msgid=f2a6ce35) with payloads
  (HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0
                                          total length : 152 ...

SEV=8 IKEDECODE/0 RPT=5093 172.18.124.241 11:40:54.250 12/05/2001 1414
                                       ( ISAKMP HEADER : ( Version 1.0
                        Initiator Cookie(8): E7 AC CD 06 A6 74 A7 1A
                        Responder Cookie(8): 98 3B 37 97 CA 06 BC 18
                                       (Next Payload : HASH (8
                                Exchange Type : Oakley Quick Mode
                                         ( Flags : 1 (ENCRYPT
                                        Message ID : f2a6ce35
                                                 Length : 52

SEV=8 IKEDBG/0 RPT=5357 172.18.124.241 11:40:54.250 12/05/2001 1421
                     : RECEIVED Message (msgid=f2a6ce35) with payloads
                       HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=5358 172.18.124.241 11:40:54.250 12/05/2001 1423
                                    [Group [rtpvpn] User [esupporttcp
                                                  processing hash

SEV=9 IKEDBG/0 RPT=5359 172.18.124.241 11:40:54.250 12/05/2001 1424
                                    [Group [rtpvpn] User [esupporttcp
                                          loading all IPSEC SAs

 SEV=9 IKEDBG/1 RPT=671 172.18.124.241 11:40:54.250 12/05/2001 1425
                                    [Group [rtpvpn] User [esupporttcp
                                           !Generating Quick Mode Key

 SEV=9 IKEDBG/1 RPT=672 172.18.124.241 11:40:54.260 12/05/2001 1426
                                    [Group [rtpvpn] User [esupporttcp
                                           !Generating Quick Mode Key

SEV=7 IKEDBG/0 RPT=5360 172.18.124.241 11:40:54.260 12/05/2001 1427
                                    [Group [rtpvpn] User [esupporttcp
                                                    :Loading subnet
                                  Dst: 0.0.0.0 mask: 0.0.0.0
                                           Src: 172.18.124.217

    SEV=4 IKE/49 RPT=58 172.18.124.241 11:40:54.260 12/05/2001 1429
                                    [Group [rtpvpn] User [esupporttcp
                      (Security negotiation complete for User (esupporttcp
     Responder, Inbound SPI = 0x70a4e243, Outbound SPI = 0x9879d238

                 SEV=9 IPSECDBG/6 RPT=283 11:40:54.260 12/05/2001 1432
,IPSEC key message parse - msgtype 1, len 620, vers 1, pid 00000000
            ,seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0
    ,spi 9879d238, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2
```

```
hmacAlg 3, lifetype 0, lifetime1 707832, lifetime2 0, dsId 0

SEV=9 IPSECDBG/1 RPT=1063 11:40:54.260 12/05/2001 1436
!Processing KEY_ADD msg

SEV=9 IPSECDBG/1 RPT=1064 11:40:54.260 12/05/2001 1437
key_msghdr2secassoc(): Enter

SEV=7 IPSECDBG/1 RPT=1065 11:40:54.260 12/05/2001 1438
No USER filter configured

SEV=9 IPSECDBG/1 RPT=1066 11:40:54.260 12/05/2001 1439
KeyProcessAdd: Enter

SEV=8 IPSECDBG/1 RPT=1067 11:40:54.260 12/05/2001 1440
KeyProcessAdd: Adding outbound SA

SEV=8 IPSECDBG/1 RPT=1068 11:40:54.260 12/05/2001 1441
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst
mask 0.0.0.0 172.18.124.217

SEV=8 IPSECDBG/1 RPT=1069 11:40:54.260 12/05/2001 1442
KeyProcessAdd: FilterIpsecAddIkeSa success

SEV=9 IPSECDBG/6 RPT=284 11:40:54.260 12/05/2001 1443
,IPSEC key message parse - msgtype 3, len 334, vers 1, pid 00000000
,seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0
,spi 70a4e243, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2
hmacAlg 3, lifetype 0, lifetime1 707832, lifetime2 0, dsId 0

SEV=9 IPSECDBG/1 RPT=1070 11:40:54.260 12/05/2001 1447
!Processing KEY_UPDATE msg

SEV=9 IPSECDBG/1 RPT=1071 11:40:54.260 12/05/2001 1448
Update inbound SA addresses

SEV=9 IPSECDBG/1 RPT=1072 11:40:54.260 12/05/2001 1449
key_msghdr2secassoc(): Enter

SEV=7 IPSECDBG/1 RPT=1073 11:40:54.260 12/05/2001 1450
No USER filter configured

SEV=9 IPSECDBG/1 RPT=1074 11:40:54.260 12/05/2001 1451
KeyProcessUpdate: Enter

SEV=8 IPSECDBG/1 RPT=1075 11:40:54.260 12/05/2001 1452
KeyProcessUpdate: success

SEV=8 IKEDBG/7 RPT=58 11:40:54.260 12/05/2001 1453
IKE got a KEY_ADD msg for SA: SPI = 0x9879d238

SEV=8 IKEDBG/0 RPT=5361 11:40:54.260 12/05/2001 1454
pitcher: rcv KEY_UPDATE, spi 0x70a4e243

SEV=4 IKE/120 RPT=58 11:40:54.260 12/05/2001 1455
172.18.124.241
[Group [rtpvpn] User [esupporttcp
(PHASE 2 COMPLETED (msgid=f2a6ce35

SEV=7 IPSECDBG/1 RPT=1076 11:40:55.120 12/05/2001 1456
!IPSec Inbound SA has received data

SEV=8 IKEDBG/0 RPT=5362 11:40:55.120 12/05/2001 1457
pitcher: recv KEY_SA_ACTIVE spi 0x709e5f39
```

```
SEV=8 IKEDBG/0 RPT=5363 11:40:55.120 12/05/2001 1458
KEY_SA_ACTIVE no old rekey centry found with new spi
0x709e5f39, mess_id 0x0
```

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل شبكة VPN من Cisco
- صفحة دعم IPSec
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).