

Configurazione di ISE 2.2 IPSEC per la comunicazione protetta e ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Architettura IPsec ISE](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione ASA](#)

[Configurazione delle interfacce ASA](#)

[Configurare il criterio IKEv1 e abilitare IKEv1 sull'interfaccia esterna](#)

[Configurazione del gruppo di tunnel \(profilo di connessione LAN a LAN\)](#)

[Configurare l'ACL per il traffico VPN di interesse](#)

[Configurare il set di trasformazioni IKEv1](#)

[Configurazione di una mappa crittografica e applicazione a un'interfaccia](#)

[Configurazione finale ASA](#)

[Configurazione di ISE](#)

[Configurazione dell'indirizzo IP in ISE](#)

[Add and to IPsec Group on ISE](#)

[Abilitare IPSEC su ISE](#)

[Verifica](#)

[ASA](#)

[ESR](#)

[ISE](#)

[Risoluzione dei problemi](#)

[Configurazione di FlexVPN da sito a sito \(da DVTI a mappa crittografica\) tra NAD e ISE 2.2](#)

[Configurazione ASA](#)

[Configurazione ESR su ISE](#)

[Considerazioni sulla progettazione di FlexVPN](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi a RADIUS IPSEC per proteggere la comunicazione con Cisco Identity Service Engine (ISE) 2.2 - Dispositivo di accesso alla rete (NAD). Il traffico RADIUS deve essere crittografato all'interno del tunnel IPsec Internet Key Exchange versione 1 e 2 (IKEv1 e IKEv2) tra Adaptive Security Appliance (ASA) e ISE. Questo documento non descrive la parte di configurazione AnyConnect SSL VPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Cisco ASA
- Concetti generali su IPSec
- Concetti generali su RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5515-X ASA con software versione 9.4(2)11
- Cisco Identity Service Engine versione 2.2
- Windows 7 Service Pack 1

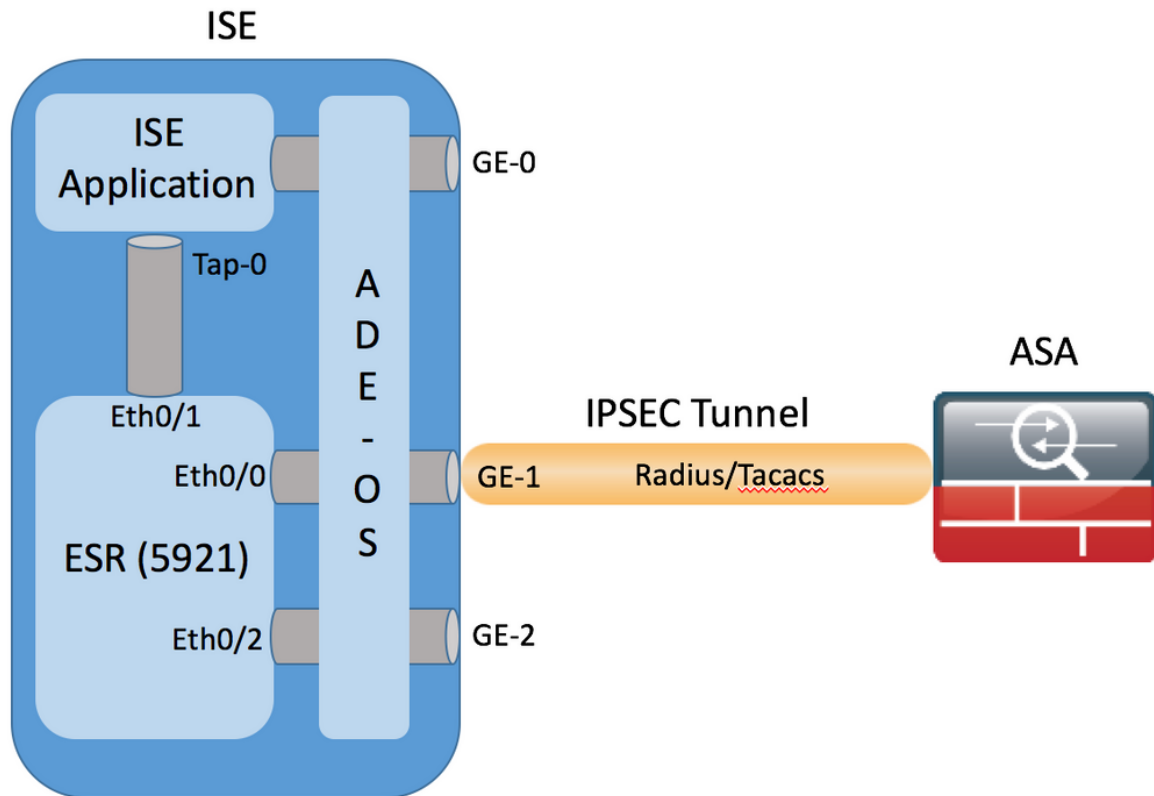
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'obiettivo è proteggere i protocolli che usano hash MD5, Radius e TACACS non sicuri con IPSec. Tenere presente quanto segue:

- Cisco ISE supporta IPSec in modalità tunnel e trasporto.
- Quando si abilita IPSec su un'interfaccia Cisco ISE, viene creato un tunnel IPSec tra Cisco ISE e NAD per proteggere la comunicazione.
- È possibile definire una chiave già condivisa o utilizzare certificati X.509 per l'autenticazione IPSec.
- È possibile abilitare IPSec sulle interfacce da Eth1 a Eth5. È possibile configurare IPSec su una sola interfaccia Cisco ISE per PSN.

Architettura IPSec ISE



Una volta ricevuti i pacchetti crittografati dall'interfaccia GE-1 ISE, ESR li intercetta sull'interfaccia Eth0/0.

```
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 10.48.26.170 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
```

ESR li decrittografa e, in base alle regole NAT preconfigurate, esegue la traduzione degli indirizzi. I pacchetti RADIUS/TACACS in uscita (verso NAD) vengono convertiti in indirizzi di interfaccia Ethernet0/0 e crittografati in seguito.

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
access-list 1 permit 10.1.1.0 0.0.0.3
```

I pacchetti destinati all'interfaccia Eth0/0 sulle porte RADIUS/TACACS devono essere inoltrati tramite l'interfaccia Eth0/1 all'indirizzo ip 10.1.1.2, che è l'indirizzo interno di ISE. Configurazione ESR di Eth0/1

```
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
```

```
no ip route-cache
```

Configurazione ISE dell'interfaccia interna Tap-0:

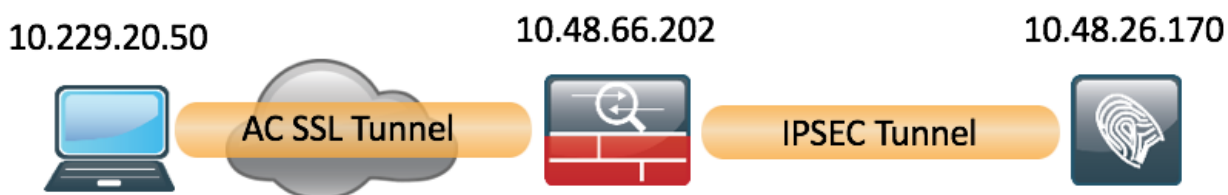
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.2 netmask 255.255.255.252 broadcast 10.1.1.3
    inet6 fe80::6c2e:37ff:fe5f:b609 prefixlen 64 scopeid 0x20<link>
    ether 6e:2e:37:5f:b6:09 txqueuelen 500 (Ethernet)
    RX packets 81462 bytes 8927953 (8.5 MiB)
    RX errors 0 dropped 68798 overruns 0 frame 0
    TX packets 105 bytes 8405 (8.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Configurazione

Questa sezione descrive come completare le configurazioni ASA CLI e ISE.

Esempio di rete

Per le informazioni di questo documento viene utilizzata la seguente configurazione della rete:



Configurazione ASA

Configurazione delle interfacce ASA

Se l'interfaccia o le interfacce ASA non sono configurate, verificare di configurare almeno l'indirizzo IP, il nome dell'interfaccia e il livello di sicurezza:

```
interface GigabitEthernet0/0
  nameif outside
  security-level 100
  ip address 10.48.66.202 255.255.254.0
```

Configurare il criterio IKEv1 e abilitare IKEv1 sull'interfaccia esterna

Per configurare i criteri Internet Security Association and Key Management Protocol (ISAKMP) per le connessioni IKEv1, immettere il comando **crypto ikev1 policy <priority>**:

```
crypto ikev1 policy 20
```

```
authentication pre-share
encryption aes
hash sha
group 5
lifetime 86400
```

Nota: esiste una corrispondenza di criteri IKEv1 quando entrambi i criteri dei due peer contengono gli stessi valori di autenticazione, crittografia, hash e parametro Diffie-Hellman. Per IKEv1, il criterio peer remoto deve inoltre specificare una durata minore o uguale alla durata del criterio inviato dall'iniziatore. Se le durate non sono identiche, l'appliance ASA usa la durata più breve.

È necessario abilitare IKEv1 sull'interfaccia che termina il tunnel VPN. In genere, si tratta dell'interfaccia esterna (o *pubblica*). Per abilitare IKEv1, immettere il comando **crypto ikev1 enable <nome-interfaccia>** in modalità di configurazione globale:

```
crypto ikev1 enable outside
```

Configurazione del gruppo di tunnel (profilo di connessione LAN a LAN)

Per un tunnel da LAN a LAN, il profilo di connessione è **ipsec-l2l**. Per configurare la chiave già condivisa IKEv1, immettere la modalità di configurazione *ipsec-attributes del gruppo di tunnel*:

```
tunnel-group 10.48.26.170 type ipsec-l2l
tunnel-group 10.48.26.170 ipsec-attributes
ikev1 pre-shared-key Krakow123
```

Configurare l'ACL per il traffico VPN di interesse

L'appliance ASA utilizza gli Access Control Lists (ACL) per distinguere il traffico da proteggere con la crittografia IPsec dal traffico che non richiede protezione. Protegge i pacchetti in uscita che corrispondono a una voce ACE (Application Control Engine) di autorizzazione e garantisce la protezione dei pacchetti in entrata che corrispondono a una voce ACE di autorizzazione.

```
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
```

Nota: un ACL per il traffico VPN usa gli indirizzi IP di origine e di destinazione dopo il protocollo NAT (Network Address Translation). L'unico traffico crittografato in questo caso è il traffico tra ASA e ISE.

Configurare il set di trasformazioni IKEv1

Un set di trasformazioni IKEv1 è una combinazione di protocolli e algoritmi di sicurezza che definiscono il modo in cui l'appliance ASA protegge i dati. Durante le negoziazioni della Security Association (SA) IPsec, i peer devono identificare un set di trasformazioni o una proposta identica per entrambi i peer. L'ASA quindi applica il set di trasformazioni o la proposta di trasformazione corrispondente per creare un'associazione di protezione (SA) che protegga i flussi di dati nell'elenco degli accessi per la mappa crittografica.

Per configurare il set di trasformazioni IKEv1, immettere il comando **crypto ipsec ikev1 transform-set:**

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

Configurazione di una mappa crittografica e applicazione a un'interfaccia

Una mappa crittografica definisce un criterio IPSec da negoziare nell'associazione di protezione IPSec e include:

- Un elenco degli accessi per identificare i pacchetti consentiti e protetti dalla connessione IPSec
- Identificazione peer
- Indirizzo locale per il traffico IPSec
- Set di trasformazioni IKEv1

Di seguito è riportato un esempio:

```
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.26.170
crypto map MAP 20 set ikev1 transform-set SET2
```

È quindi possibile applicare la mappa crittografica all'interfaccia:

```
crypto map MAP interface outside
```

Configurazione finale ASA

Di seguito è riportata la configurazione finale dell'appliance ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.48.66.202 255.255.254.0
!
!
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
!
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
!
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.26.170
crypto map MAP 20 set ikev1 transform-set SET2
crypto map MAP interface outside
```

Configurazione di ISE

Configurazione dell'indirizzo IP in ISE

L'indirizzo deve essere configurato sull'interfaccia GE1-GE5 dalla CLI. GE0 non è supportato.

```
interface GigabitEthernet 1
 ip address 10.48.26.170 255.255.255.0
 ipv6 address autoconfig
 ipv6 enable
```

Nota: L'applicazione viene riavviata dopo la configurazione dell'indirizzo IP sull'interfaccia:

% La modifica dell'indirizzo IP potrebbe causare il riavvio dei servizi ISE
Continuare con la modifica dell'indirizzo IP? S/N [N]: Y

Add and to IPsec Group on ISE

Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**. Fare clic su **Add**. Assicurarsi di configurare il nome, l'indirizzo IP e il segreto condiviso. Per terminare il tunnel IPsec da NAD, selezionare **YES (S)** in IPSEC Network Device Group (Gruppo dispositivi di rete IPSEC).

The screenshot displays the 'Network Devices' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is titled 'Network Devices List > EK_ASA'. The main configuration area is titled 'Network Devices' and contains the following fields and options:

- Name:** EK_ASA (highlighted with a red box)
- Description:** (empty field)
- * IP Address:** 10.48.66.202 / 32
- * Device Profile:** Cisco (dropdown menu)
- Model Name:** (dropdown menu)
- Software Version:** (dropdown menu)
- * Network Device Group:**
 - Device Type:** All Device Types (dropdown menu)
 - IPSEC:** Yes (dropdown menu, highlighted with a red box)
 - Location:** All Locations (dropdown menu)
- RADIUS Authentication Settings:** (checked checkbox)
 - RADIUS UDP Settings:**
 - Protocol:** RADIUS
 - * Shared Secret:** (password field, highlighted with a red box)
 - CoA Port:** 1700

Dopo aver aggiunto l'NAD, occorre creare un percorso aggiuntivo sull'ISE per garantire che il traffico RADIUS passi attraverso l'ESR e venga criptato:

```
ip route 10.48.66.202 255.255.255.255 gateway 10.1.1.1
```

Abilitare IPSEC su ISE

Selezionare **Amministrazione > Sistema > Impostazioni**. Fare clic su **Radius** e quindi su **IPSEC**. Selezionare PSN (Single/Multiple/All), selezionare l'opzione **Abilita**, selezionare l'interfaccia e selezionare il metodo di autenticazione. Fare clic su **Salva**. A questo punto, i servizi verranno riavviati nel nodo selezionato.

Notare che dopo il riavvio dei servizi, la configurazione della CLI di ISE mostra l'interfaccia configurata senza indirizzo IP e nello stato shutdown, è previsto che il router ESR (Embedded Services Router) prenda il controllo dell'interfaccia ISE.

```
interface GigabitEthernet 1
 shutdown
 ipv6 address autoconfig
 ipv6 enable
```

Dopo il riavvio dei servizi, la funzionalità ESR è abilitata. Per accedere a ESR digitare esr nella riga di comando:

```
ISE22-1ek/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.
```

Press RETURN to get started, <CTRL-C> to exit

```
ise-esr5921>en
ise-esr5921#
```

ESR è dotato della seguente configurazione crittografica:

```
crypto keyring MVPN-spokes
```



```

pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
!
crypto isakmp policy 10
  encr aes
  hash sha256
  authentication pre-share
  group 16
!
crypto isakmp policy 20
  encr aes
  hash sha256
  authentication pre-share
  group 14
!
crypto isakmp key Krakow123 address 0.0.0.0
!
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
  mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
  mode transport
!
crypto dynamic-map MVPN-dynmap 10
  set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap

```

Poiché ASA non supporta l'algoritmo di hashing sha256, è necessaria una configurazione aggiuntiva su ESR per soddisfare i criteri IKEv1 per la prima e la seconda fase di IPSEC. Configurare il criterio isakmp e il set di trasformazioni in modo che corrispondano a quelli configurati sull'appliance ASA:

```

crypto isakmp policy 30
  encr aes
  authentication pre-share
  group 5
!
crypto ipsec transform-set radius-3 esp-aes esp-sha-hmac
  mode tunnel
!
crypto dynamic-map MVPN-dynmap 10
  set transform-set radius radius-2 radius-3

```

Verificare che l'ESR disponga di un percorso per l'invio dei pacchetti crittografati:

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

Verifica

ASA

Prima della connessione dei client Anyconnect, l'ASA non ha sessioni crittografiche:

```
BSNS-ASA5515-11# sh cry isa sa
```

There are no IKEv1 SAs

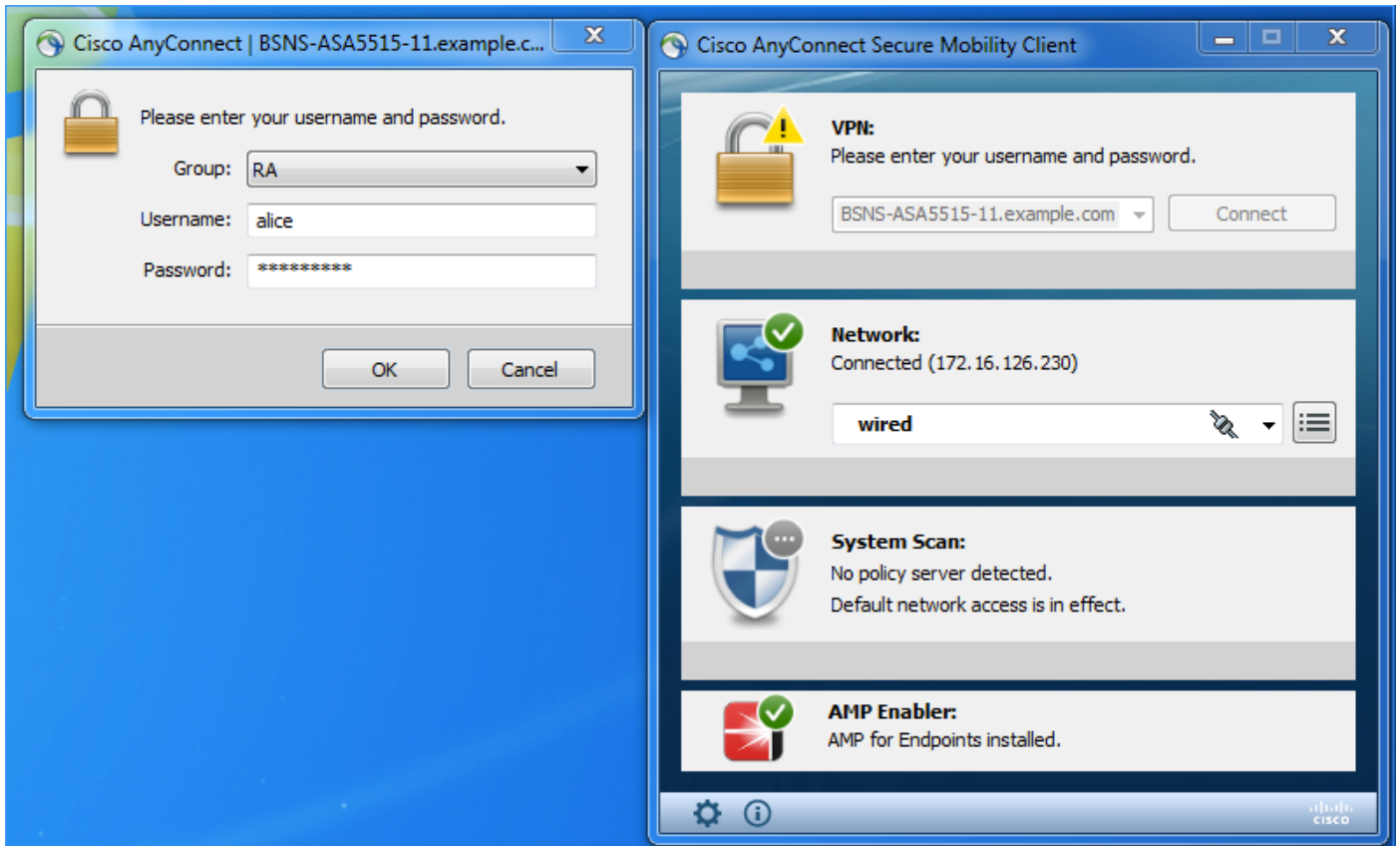
There are no IKEv2 SAs

```
BSNS-ASA5515-11# sh cry ipsec sa
```

There are no ipsec sas

```
BSNS-ASA5515-11#
```

Il client si connette tramite il client VPN Anyconnect, come origine di autenticazione per l'ISE 2.2.



ASA invia un pacchetto Radius, che attiva la creazione della sessione VPN, una volta attivo il tunnel. L'output seguente viene visualizzato sull'appliance ASA e conferma che la fase 1 del tunnel è attiva:

```
BSNS-ASA5515-11# sh cry isa sa
```

IKEv1 SAs:

```
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: 10.48.26.170
  Type      : L2L           Role      : initiator
  Rekey     : no           State     : MM_ACTIVE
```

There are no IKEv2 SAs

```
BSNS-ASA5515-11#
```

La fase 2 è attiva e i pacchetti vengono crittografati e decrittografati:

```
BSNS-ASA5515-11# sh cry ipsec sa
interface: outside
```

Crypto map tag: MAP, seq num: 20, local addr: 10.48.66.202

access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
local ident (addr/mask/prot/port): (10.48.66.202/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.48.26.170/255.255.255.255/0/0)
current_peer: 10.48.26.170

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 5, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.48.66.202/0, remote crypto endpt.: 10.48.26.170/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 5BBE9F07
current inbound spi : 068C04D1

inbound esp sas:

spi: 0x068C04D1 (109839569)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 323584, crypto-map: MAP
sa timing: remaining key lifetime (kB/sec): (4373999/3558)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003F

outbound esp sas:

spi: 0x5BBE9F07 (1539219207)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 323584, crypto-map: MAP
sa timing: remaining key lifetime (kB/sec): (4373999/3558)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ESR

Le stesse uscite possono essere controllate con l'ESR, la prima fase è attiva:

```
ise-esr5921#sh cry isa sa
```

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	status
10.48.26.170	10.48.66.202	QM_IDLE	1012	ACTIVE MVPN-profile

```
IPv6 Crypto ISAKMP SA
```

```
ise-esr5921#
```

La fase 2 è attiva, i pacchetti vengono crittografati e decrittografati correttamente:

```
ise-esr5921#sh cry ipsec sa
```

```
interface: Ethernet0/0
```

```
  Crypto map tag: radius, local addr 10.48.26.170
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (10.48.26.170/255.255.255.255/0/0)
```

```
remote ident (addr/mask/prot/port): (10.48.66.202/255.255.255.255/0/0)
```

```
current_peer 10.48.66.202 port 500
```

```
  PERMIT, flags={}
```

```
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
```

```
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.48.26.170, remote crypto endpt.: 10.48.66.202
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
```

```
current outbound spi: 0x68C04D1(109839569)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0x5BBE9F07(1539219207)
```

```
  transform: esp-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 31, flow_id: SW:31, sibling_flags 80000040, crypto map: radius
```

```
  sa timing: remaining key lifetime (k/sec): (4259397/3508)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x68C04D1(109839569)
```

```
  transform: esp-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 32, flow_id: SW:32, sibling_flags 80000040, crypto map: radius
```

```
  sa timing: remaining key lifetime (k/sec): (4259397/3508)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

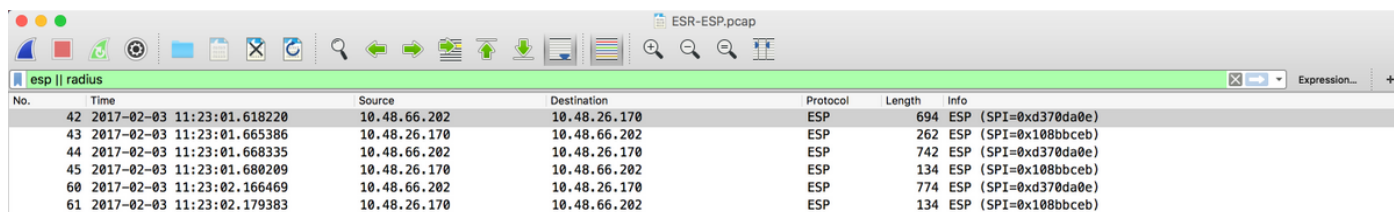
ISE

L'autenticazione in tempo reale indica un'autenticazione PAP_ASCII regolare:

The screenshot shows the Cisco ISE Live Logs interface. At the top, there are navigation tabs for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below the navigation, there are several summary cards for various metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (0). Below these cards, there is a table of authentication logs. The table has columns for Time, Status, Details, Repeat, Identity, Endpoint ID, Endpoint Prof, Authenticator, Authorizati..., Authorizati..., IP Address, Network Device, Device Port, Identity Group, and Posture St... The table shows two entries for the user 'alice' on Feb 03, 2017 at 11:23:02.174 AM and 11:23:01.684 AM. Both entries show a status of 'Success' and a repeat count of 0. The authentication method is PAP_ASCII and the authorization is PermitAccess.

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture St...
Feb 03, 2017 11:23:02.174 AM	Success		0	alice	00:0C:29:C9:D9:37	Workstation	Default >> D...	Default >> B...	PermitAccess	10.10.10.12				
Feb 03, 2017 11:23:01.684 AM	Success		0	alice	00:0C:29:C9:D9:37	Workstation	Default >> D...	Default >> B...	PermitAccess		EK_ASA		Workstation	

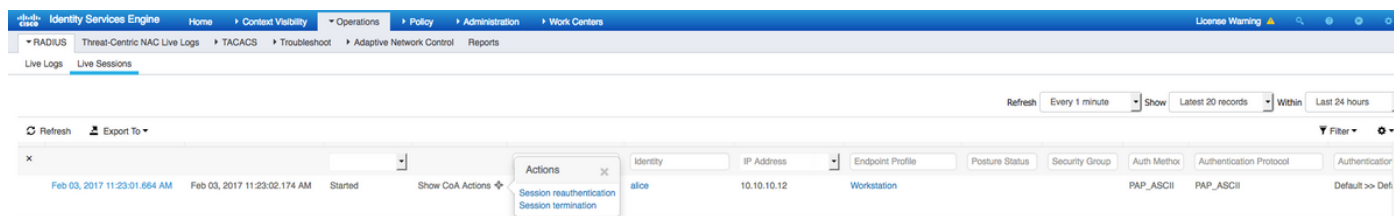
Le immagini acquisite tramite l'interfaccia GE1 di ISE e filtrate con ESP o Radius, confermano che il testo non è crittografato e che il traffico è interamente crittografato:



The screenshot shows a network traffic capture window titled 'ESR-ESP.pcap'. The filter is set to 'esp || radius'. The table below lists several captured packets, all of which are ESP (Encapsulating Security Payload) packets. The source and destination IP addresses are 10.48.66.202 and 10.48.26.170. The protocols are all ESP, and the lengths vary between 694 and 134 bytes. The information column shows SPI values like 0xd370da0e and 0x108bbceb.

No.	Time	Source	Destination	Protocol	Length	Info
42	2017-02-03 11:23:01.618220	10.48.66.202	10.48.26.170	ESP	694	ESP (SPI=0xd370da0e)
43	2017-02-03 11:23:01.665386	10.48.26.170	10.48.66.202	ESP	262	ESP (SPI=0x108bbceb)
44	2017-02-03 11:23:01.668335	10.48.66.202	10.48.26.170	ESP	742	ESP (SPI=0xd370da0e)
45	2017-02-03 11:23:01.680209	10.48.26.170	10.48.66.202	ESP	134	ESP (SPI=0x108bbceb)
60	2017-02-03 11:23:02.166469	10.48.66.202	10.48.26.170	ESP	774	ESP (SPI=0xd370da0e)
61	2017-02-03 11:23:02.179383	10.48.26.170	10.48.66.202	ESP	134	ESP (SPI=0x108bbceb)

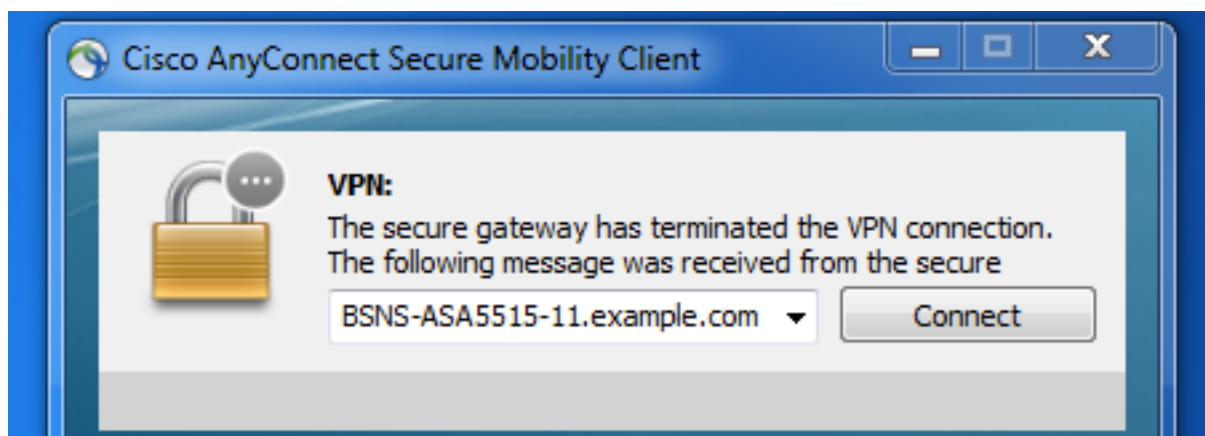
È anche possibile inviare pacchetti criptati da ISE - Change of Authorization (CoA) - una volta che il tunnel è operativo:



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The 'Live Sessions' tab is active, displaying a table of sessions. One session is highlighted, showing the user 'alice' with IP address '10.10.10.12'. The session is in a 'Started' state. An 'Actions' menu is open, showing options for 'Session reauthentication' and 'Session termination'. The 'Session termination' option is selected, indicating that the session has been terminated.

Time	Source	Destination	Protocol	Length	Info
Feb 03, 2017 11:23:01.664 AM	Feb 03, 2017 11:23:02.174 AM	Started	alice	10.10.10.12	Workstation

Nell'esempio riportato sotto, è stata emessa la terminazione della sessione e di conseguenza il client VPN è stato disconnesso:



Risoluzione dei problemi

Per risolvere i problemi relativi a IPSEC, è possibile applicare le tecniche comuni di risoluzione dei problemi delle VPN. Di seguito sono riportati alcuni documenti utili:

[Nota tecnica sulla risoluzione dei problemi relativi ai debug IOS IKEv2 per la VPN da sito a sito con PSK](#)

[Debug ASA IKEv2 per VPN da sito a sito con PSK](#)

[Risoluzione dei problemi IPsec: descrizione e uso dei comandi di debug](#)

Configurazione di FlexVPN da sito a sito (da DVTI a mappa crittografica) tra NAD e ISE 2.2

È inoltre possibile proteggere il traffico RADIUS con FlexVPN. Nell'esempio seguente viene utilizzata la topologia seguente:

Interface inside

172.16.0.1



IPSEC Tunnel

Radius/Tacacs

10.48.17.87



Interface outside

10.48.66.202

Interface Tap0 – 10.1.1.2

La configurazione di FlexVPN è semplice. Per maggiori informazioni:

<http://www.cisco.com/c/en/us/support/docs/security/flexvpn/116008-flexvpn-nge-config-00.html>

Configurazione ASA

```
hostname BSNS-ASA5515-11
domain-name example.com

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 10.48.66.202 255.255.254.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.0.1 255.255.255.0
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network POOL
 subnet 10.10.10.0 255.255.255.0
object network ISE
 host 10.48.17.86
object network ISE22
 host 10.1.1.2
object network INSIDE-NET
 subnet 172.16.0.0 255.255.0.0
access-list 101 extended permit ip host 172.16.0.1 host 10.1.1.2
access-list OUT extended permit ip any any
nat (inside,outside) source static INSIDE-NET INSIDE-NET destination static ISE22 ISE22
nat (outside,outside) source dynamic POOL interface
nat (inside,outside) source dynamic any interface
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.48.66.1 1

aaa-server ISE22 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE22 (inside) host 10.1.1.2
 key *****
```

```
crypto ipsec ikev2 ipsec-proposal SET
  protocol esp encryption aes
  protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map DMAP 1 set ikev1 transform-set SET
crypto map MAP 10 ipsec-isakmp dynamic DMAP
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.17.87
crypto map MAP 20 set ikev2 ipsec-proposal SET
crypto map MAP interface outside
crypto ikev2 policy 10
  encryption aes
  integrity sha256
  group 2
  prf sha256
  lifetime seconds 86400
crypto ikev2 enable outside
management-access inside
webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-4.4.00243-webdeploy-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable
group-policy GP-SSL internal
group-policy GP-SSL attributes
  vpn-tunnel-protocol ssl-client
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  address-pool POOL
  authentication-server-group ISE22
  accounting-server-group ISE22
  default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
  group-alias RA enable
tunnel-group 10.48.17.87 type ipsec-l2l
tunnel-group 10.48.17.87 ipsec-attributes
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****
```

Configurazione ESR su ISE

```
ise-esr5921#sh run
Building configuration...

Current configuration : 5778 bytes
!
! Last configuration change at 17:32:58 CET Thu Feb 23 2017
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service call-home
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
!
```

```

!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
clock timezone CET 1 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
no destination transport-method email
!
!
!
!
!
!
!

!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191

```



```
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
```

quit

```
license udi pid CISCO5921-K9 sn 98492083R3X
username lab password 0 lab
!
redundancy
!
!
!
crypto keyring MVPN-spokes
  pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
crypto ikev2 authorization policy default
  route set interface
  route set remote ipv4 10.1.1.0 255.255.255.0
!
!
!
crypto ikev2 keyring mykeys
  peer ISR4451
  address 10.48.23.68
  pre-shared-key Krakow123
!
!
!
crypto ikev2 profile default
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local mykeys
  aaa authorization group psk list default default local
  virtual-template 1
!
!
crypto isakmp policy 10
  encr aes
  hash sha256
  authentication pre-share
  group 16
!
crypto isakmp policy 20
  encr aes
  hash sha256
  authentication pre-share
  group 14
crypto isakmp key Krakow123 address 0.0.0.0
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
```

```

mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
!
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
!
!
!
!
interface Loopback0
ip address 10.1.12.2 255.255.255.0
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 10.48.17.87 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
description e0/2->connection to CSSM backend license server
no ip address
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/3
no ip address
shutdown
!
interface Virtual-Templatel type tunnel
ip unnumbered Loopback0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile default
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
ip route 0.0.0.0 0.0.0.0 10.48.17.1
!
!

```

```
!  
access-list 1 permit 10.1.1.0 0.0.0.3  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
line con 0  
  logging synchronous  
line aux 0  
line vty 0 4  
  login  
  transport input none  
!  
!  
end
```

Considerazioni sulla progettazione di FlexVPN

- Il tunnel VPN è costruito utilizzando la tecnologia DVTI sul lato ESR e la mappa crittografica sull'appliance ASA, con la configurazione sopra descritta, è in grado di generare il pacchetto Radius proveniente dall'interfaccia interna, che garantirà la corretta lista degli accessi per la crittografia, in modo da attivare la creazione di sessioni VPN.
- Notare che in questo caso, l'ASA e l'AD devono essere definiti sull'ISE con l'indirizzo IP dell'interfaccia interna.