Seminario
Collegamenti VPN: algoritmi e principi di funzionamento

Università di Bologna
DEIS – Laboratorio di Reti di Telecomunicazioni T
11 maggio 2011

Ing. Vincenzo Vaccarino
Dipartimento Sistemi e Tecnologie - Settore Operazioni
CINECA

Agenda

- Cosa è il CINECA
- Accesso remoto e Crittografia
- VPN IPsec
- Esempi di configurazione
  - Site to Site
  - via client

Agenda

- Cosa è il CINECA
- Accesso remoto e Crittografia
- VPN IPsec
- Esempi di configurazione
  - Site to Site
  - via client

CINECA

- Nasce nel 1969
- La prima funzione è la condivisione delle risorse di calcolo fra gli atenei consorziati
- Negli anni successivi si sviluppano ulteriori attività di supporto ai consorziati, il cui numero aumenta progressivamente

50 atenei:

Bari, Politecnico di Bari, Basilicata, Bergamo, Bologna, Brescia, Calabria, Camerino, Catania, Cassino Chieti, Enna, Ferrara, Firenze, Genova, Insubria, L'Aquila, Macerata, Messina, Milano Bicocca, Politecnico di Milano, Modena e Reggio Emilia, Molise, Seconda Università di Napoli, Napoli Federico II, Padova, Parma, Pavia, Perugia, Pisa, Politecnica delle Marche, Roma Tre, Roma La Sapienza, Mediterranea di Reggio Calabria, Salerno, Sannio, Sassari, Siena, Trento, Trieste, Torino, Politecnico di Torino, Udine, Urbino, Venezia Cà Foscari, Iuav di Venezia, Verona

il CNR
l'OGS
Il MiUR

Attività istituzionali

- Calcolo ad alte prestazioni, per utenze pubbliche (accademiche) e private
- Servizi gestionali a supporto delle Università
- Servizi gestionali a supporto del MIUR
- Partecipazione a progetti europei: DEISA2, PRACE, HPC-Europa, etc…

Attività istituzionali

Trasferimento tecnologico verso:

- Pubblica Amministrazione ed Enti Locali
- Sanità
- Industrie
- Unione Europea

Altre attività

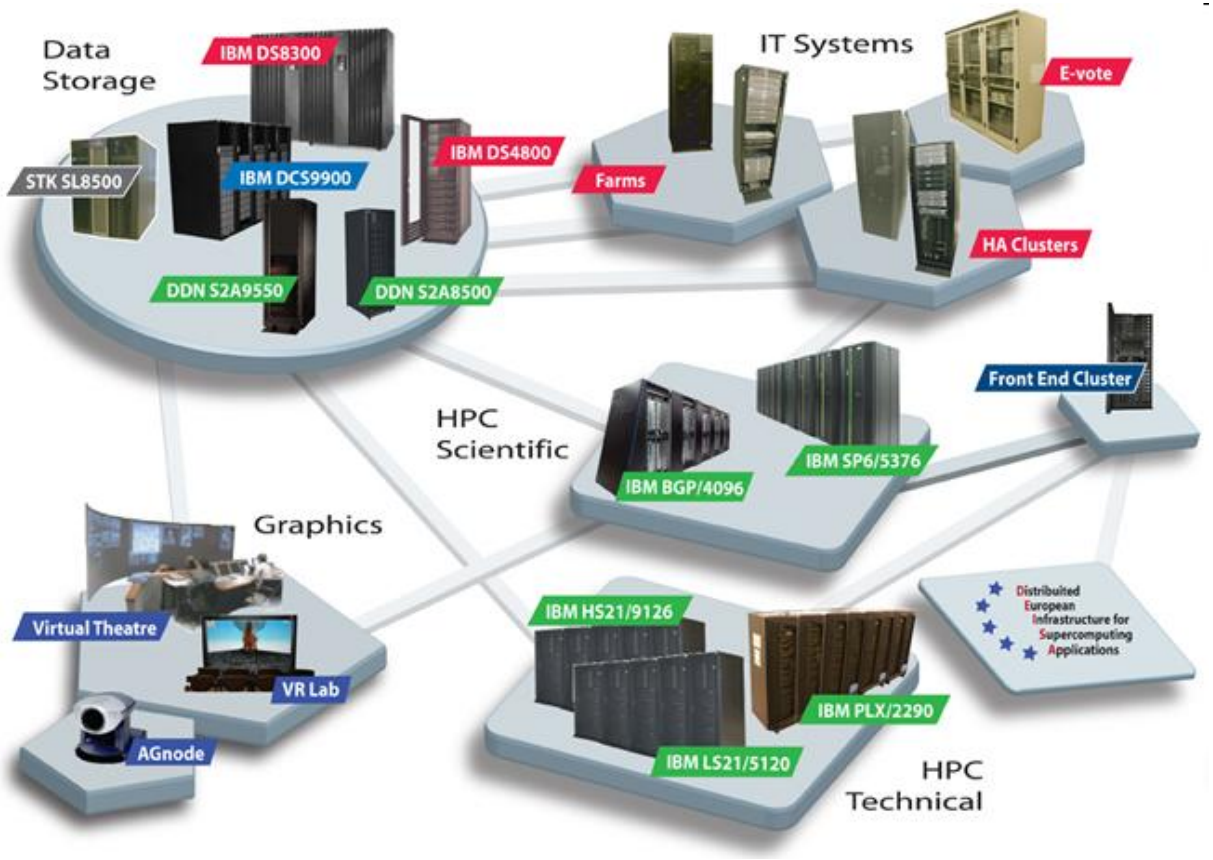
Servizi commerciali:

- Hosting e housing per clienti privati (Datacenter commerciale)

Laboratori

- TV Digitale, servizi multimediali, E-learning

Risorse del Cineca



Risorse del Cineca

- **Sistemi ad alte prestazioni:** supercalcolatori a supporto della ricerca scientifica e tecnologica

- **Sistemi "mission critical”:** sistemi IT per i servizi che richiedono sicurezza, continuità ed efficienza nelle prestazioni

- **Sistema di memorizzazione dati**: un'avanzata Storage Area Network collegata tramite fiber channel ai sistemi di calcolo veri e propri

- **Grafica e Realtà virtuale**: tecnologie innovative a supporto della Visualizzazione scientifica e della Grafica tridimensionale immersiva

- **Access Grid Node**: un’infrastruttura consente l'interazione audiovisiva a distanza tra gruppi di persone anche molto numerosi.

Qualche numero

Risorse umane : oltre 350 dipendenti

Presente nella classifica dei 500 centri di supercalcolo mondiali per potenza di calcolo installata

Cluster Power 575 da 5376 processori

Qualche numero

Nell'ambito del progetto PRACE (Partnership for Advanced Computing in Europe)

- Cluster SP6, potenza di picco 100 Teraflops, storage 1,5 Petabyte
- Cluster Blue Gene P (15 Tflops) per sperimentazione
- Cluster Blue Gene Q (1 Pflops), a partire dal 2011/2012

Infrastruttura di rete

CINECA ha recentemente intrapreso un progetto di miglioramento della propria infrastruttura di rete, che ha visto una completa riprogettazione della stessa

Il progetto ha ricevuto uno dei premi del Computerworld Honors Program per il 2008

Riferimenti online

Sito istituzionale

http://www.cineca.it

Riferimenti sulle strutture di supercalcolo e di rete

http://www.top500.org
http://www.top500.org/sites/273
http://www.cwhonors.org/laureates/2008laureates.htm
http://www.cwhonors.org/viewCaseStudy2008.asp?NominationID=722

Agenda

- Cosa è il CINECA
- Accesso remoto e Crittografia
- VPN IPsec
- Esempi di configurazione
  - Site to Site
  - via client

Accesso remoto

- Esigenza tipica delle strutture distribuite
- Accesso remoto con uguali modalità rispetto a quello locale
- Connettività basata su policy dalle sedi distaccate
- Utilizzo di connessioni via Internet, non “dedicate”
- Possibilità di utilizzo anche per il telelavoro

Accesso remoto: vantaggi

- Possibilità di interconnessione fra sedi remote
- Maggiore flessibilità di connessione (geografica e organizzativa)
- Maggiore efficienza del personale
- Policy unica di sicurezza
- Maggior numero di servizi che usano le stesse interconnessioni

Accesso remoto: problemi

- Ambiente di rete di cui non si ha pieno controllo
- Necessità di controllare la sicurezza, l'autenticità e l'integrità dei dati in transito
- Necessità di integrare il sistema di comunicazione con gli apparati di sicurezza presenti
- Problema dell'autenticazione dell'interlocutore

Accesso remoto: soluzione VPN

- La VPN IPsec garantisce la sicurezza della comunicazione
- Il firewall locale (o le access-list sui router) fornisce le policy di accesso alle risorse
- Il protocollo è basato su standard aperti
- Permette di garantire la sicurezza, l'autenticazione e l'integrità

Crittografia

- La crittografia ha lo scopo di rendere un messaggio leggibile solo da parte di chi è autorizzato a farlo

- In generale si compone di un algoritmo (eventualmente una funzione matematica) e di una o più “chiavi”

- In informatica si distinguono crittografia simmetrica e asimmetrica

Crittografia

- Lo sviluppo della crittografia è soprattutto stato legato ad esigenze politiche e militari

- I primi cifrari noti risalgono all'antica Grecia e a Cesare

- Gli attacchi per "sfondare" una codifica si distinguono in analitici e "brute force"
  - Brute force consiste nel provare tutte le possibili varianti
  - Gli attacchi analitici si basano invece sulla possibilità di provare un numero di varianti inferiore a quello massimo

Crittografia simmetrica

- La stessa chiave viene usata sia per criptare che per decriptare il messaggio
- Si basa quindi sulla segretezza di tale chiave di codifica, che deve essere conosciuta solo e soltanto da coloro che sono autorizzati
- In linea di principio permette di assicurare la riservatezza del messaggio, ma non di autenticare l'identità del mittente

Crittografia simmetrica: comparazione

Valutazione della robustezza degli algoritmi di criptazione simmetrica

Livello sicurezza	Complessità	Algoritmi
Molto debole	O (2^40)	DES, MD5
Debole	O (2^64)	RC4, SHA-1
Normale	O (2^80)	3DES
Standard	O (2^128)	AES-128, SHA-256
Alto	O (2^192)	AES-192, SHA-384
Altissimo	O (2^256)	AES-256, SHA-512

Algoritmi: DES

- DES è un algoritmo a chiave simmetrica, nato nel 1976
- Si basa su una chiave di lunghezza (utile) di 56 bit
- Oggi non è più considerato sicuro, in quanto è possibile violarlo in meno di 24 ore, con attacchi di tipo brute force
- E' stato sostituito, come standard diffuso, prima da 3DES, poi da AES

Algoritmi: DES (principi)

- Il messaggio originale è diviso in blocchi di 64 bit, processati separatamente

- Il blocco viene diviso in due blocchi di 32 bit, sottoposti a 16 stadi di elaborazione, in ognuno dei quali viene applicata una parte della chiave di criptazione e poi combinati con operatori XOR

- La decodifica avviene semplicemente invertendo l'ordine delle operazioni svolte in codifica

Algoritmi: 3DES

- 3DES è basato (ovviamente) su DES, ed è stato creato nel 1978
- Si basa su 3 applicazioni successive dell'algoritmo DES, con chiavi che possono essere uguali tra loro o diverse
- La chiave risulta quindi pari a 3 volte quella DES (in teoria 168 bit, nella pratica dipende dalla scelta delle chiavi, di solito 112 bit)
- E' considerato ancora piuttosto sicuro, se le chiavi per le 3 fasi sono fra loro diverse

Algoritmi: AES

- AES è stato formalizzato nel 2001 dopo 5 anni di discussioni
- E' il protocollo di criptazione standard del governo USA
- L'algoritmo discende dall'algoritmo Rijndael, ma tratta blocchi fissi di 128 bit
- Le chiavi possono essere di 128, 192, 256 bit, ma già le prime sono ad oggi ancora considerate sicure

Crittografia asimmetrica

- Le chiavi vengono generate a coppie, con funzioni diverse, e denominate chiave pubblica e privata

- La chiave pubblica è destinata ad avere la maggiore diffusione possibile, quella privata deve essere conservata dal solo proprietario

- Questo schema di principio permette di verificare l'identità del mittente (e insieme alle funzioni di hash, l'integrità del messaggio)

Crittografia comparazione

Confronto fra le lunghezze delle chiavi, a parità di complessità

Chiave simmetrica	Chiave asimmetrica
80	1024
112	2048
128	3072
192	7680
256	15360

Crittografia asimmetrica

- Ogni utente genera due chiavi, tra loro correlate, denominate chiave pubblica (Pu) e chiave privata (Pr)
- Il principio di funzionamento è che la conoscenza della chiave pubblica e dell'algoritmo non permetta di risalire alla chiave privata
- La chiave pubblica cripta i dati e verifica le "firme"
- La chiave privata decripta i dati e "firma" i messaggi

Crittografia asimmetrica

- E' ideale per i canali non sicuri e quando sia poco pratico scambiarsi fisicamente le chiavi
- In linea di principio, rimane il problema di autenticare la chiave pubblica che si può magari trovare su un server Internet
- Il principio di funzionamento è che la coppia di chiavi viene creata sulla base di un'operazione facile, ma difficilmente "invertibile"
- Nel 2005, si poteva cercare di sfondare una chiave di 660 bit, ma le chiavi comunemente usate sono di 1024-2048 bit

Crittografia asimmetrica

- Il funzionamento di principio vede due utenti, A e B, che devono scambiarsi il messaggio M, su un canale “non sicuro”

- Ognuno di loro genera una coppia di chiavi, Pua e Pra per l’utente A, e Pub e Prb per l’utente B

- Queste chiavi sono correlate in modo che Pu(Pr(M)) = M e Pr(Pu(M)) = M

- Ogni utente conosce le chiavi pubbliche dell’altro utente

Crittografia asimmetrica: sicurezza

- Se B cripta il messaggio M con la chiave Pua, che conosce, ottiene un messaggio Pua(M), che solo la chiave Pra può decriptare

- In questo modo si garantisce la riservatezza: solo il destinatario può decifrare il messaggio in chiaro

- L'intercettazione del messaggio criptato non ne permette la decifratura, perché nessuno possiede la chiave Pra

Crittografia asimmetrica: autenticazione

- Se B invece cripta il messaggio M con la chiave Prb, ottiene un messaggio Prb(M), che solo la chiave Pub può decriptare

- La chiave è però conoscibile da chiunque, ma la decriptazione riesce solo se la criptazione è stata fatta dall'unico utente che conosce Prb

- In questo modo si garantisce la riconoscibilità del mittente

Crittografia asimmetrica: integrità

- In realtà non serve criptare due volte il messaggio con due chiavi diverse, visto che una delle due non aumenta la riservatezza

- La firma quindi, avviene in forma di criptazione di un digest (hash) ottenuto dal messaggio

- Il destinatario, decifrando l'hash, oltre ad assicurarsi sull'identità del mittente, può calcolare l'hash del messaggio ricevuto, per verificare anche l'integrità del messaggio

Controllo di integrità

- Per il controllo di integrità si sfrutta il principio della criptazione con chiave privata, ma su un blocco di dati di lunghezza limitata

- A partire dal messaggio, mediante una funzione di hash, si ottiene un digest di lunghezza finita, che viene criptato con la chiave privata

- Il destinatario, decodificando l'hash, oltre ad assicurarsi sull'identità del mittente, può a sua volta calcolare l'hash del messaggio ricevuto, per verificarne anche l'integrità

Funzioni di hash

- Una funzione di hash è una funzione che, a partire da un messaggio qualsiasi M, fornisce una stringa di lunghezza finita D, dipendente dal contenuto di M

- Una modifica minima al messaggio M fornirebbe un digest D', completamente diverso da D

- Maggiore è la lunghezza di D, maggiore è la possibilità di avere hash diversi per messaggi diversi

Funzioni di hash

- La lunghezza finita di D impedisce di avere corrispondenza biunivoca

- Ci si affida quindi alla “resistenza alle collisioni”, ossia alla difficoltà di ottenere:
  - Un messaggio M’ che abbia lo stesso hash di uno dato M
  - Due messaggi M e M’ che abbiano lo stesso hash

- La debolezza di un algoritmo si evidenzia quando è possibile creare messaggi con collisioni

Funzioni di hash: MD5

- MD5 (Message Digest algorithm 5) viene creato nel 1991
- Genera stringhe di 128 bit
- Nel 1995 e 1996 vengono trovate le prime collisioni
- A partire dal 2004, diversi attacchi portarono a generare collisioni, o addirittura certificati diversi con gli stessi hash, in tempi “ragionevoli”

Funzioni di hash: SHA-1

- SHA-1 fa parte di una famiglia di algoritmi (SHA = Secure Hash Algorithm) e viene pubblicato nel 1995
- Genera stringhe di 160 bit (le versioni successive SHA-2 hanno diverse lunghezze)
- E' uno standard usato in diversi protocolli di sicurezza, SSL, PGP, SSH, IPsec, etc.
- Dal 2004-2005 sono state annunciate varie possibilità di trovare collisioni per questa funzione, comunque ancora utilizzata

Agenda

- Cosa è il CINECA
- Accesso remoto e Crittografia
- VPN IPsec
- Esempi di configurazione
  - Site to Site
  - via client

VPN IPsec

- VPN significa Virtual Private Network
- Si tratta di una rete gerarchicamente locale
- Utilizza come connettività le normali connessioni Internet
- Esistono sia reti “Site-to-site”, sia connessioni “da client”
- IPsec è un protocollo di sicurezza usato su questo tipo di connessioni potenzialmente “a rischio”

Protocollo IPsec

- Protocollo normato dagli standard IETF
- Comprende standard aperti
- Utilizza la crittografia per
  - Autenticazione dei pacchetti IP
  - Verifica dell'integrità del contenuto di ogni pacchetto
  - Confidenzialità del contenuto dei pacchetti

Protocollo IPsec: caratteristiche

- Confidenzialità : ogni pacchetto viene criptato prima di essere trasmesso su una rete non sicura

- Integrità : il destinatario può verificare che il contenuto del pacchetto non sia stato modificato

- Autenticazione : il destinatario può autenticare il mittente di un pacchetto inviato

- Anti-replay : si può verificare che ogni pacchetto sia unico

IPsec (protocolli)

- IKE (Internet Key Exchange) è il protocollo che permette lo scambio delle chiavi di criptazione

- ESP (Encapsulation Security Payload) è il protocollo che si occupa della criptazione, dell'autenticazione e della sicurezza dei dati

- AH (Authentication Header) fornisce le strutture per l'autenticazione e la verifica della sicurezza dei dati

IPsec (protocolli)

- La criptazione in IPsec avviene con algoritmi simmetrici
- IKE deve quindi fornire un sistema sicuro per scambiare le chiavi per le successive fasi di criptazione
- Come algoritmi di criptazione e hash, IPsec utilizza
  - DES, 3DES, AES
  - HMAC, MD5, SHA-1
- Quali algoritmi siano usati, viene definito in fase di negoziazione

Autenticazione del peer

- L'identificazione del router remoto con cui si stabilisce una connessione può avvenire in diversi modi:

  - Username e password
  - One Time Password
  - Metodi biometrici
  - Chiave condivisa (preshared key)
  - Certificato digitale

IKE: principi di funzionamento

- IKE utilizza l'algoritmo di scambio Diffie-Hellman per generare una coppia di chiavi simmetriche, da usare poi per criptare il traffico

- Il metodo usato è di tipo asimmetrico, per evitare che non autorizzati possano individuare le chiavi

- Per altri parametri di sicurezza, come dati da proteggere, robustezza delle chiavi, metodi di hash, etc. si usa la porta UDP 50

IKE: principi di funzionamento

- Per negoziare una SA (associazione di sicurezza), sono necessari:

  - ISAKMP – architettura dello scambio di messaggi (formato dei pacchetti, policy di sicurezza)
  - SKEME – protocollo per utilizzare la criptazione a chiave pubblica per autenticare
  - Oakley – protocollo per lo scambio di chiavi

IKE: principi di funzionamento

- I parametri gestiti dallo scambio IKE per la SA:
  - Tempo di vita della SA
  - Cambio delle chiavi di criptazione a sessione in corso
  - Autenticazione dinamica dei peer
  - Supporto per le Certification Authority

IKE: fasi

La sessione IKE si compone di tre fasi (massimo)

- Fase 1 – autenticazione dei peer e negoziazione delle SA (può avvenire con due diverse modalità): transform set, hash, etc.

- Fase 1.5 (solo per i client) – autenticazione tramite protocollo Xauth, invio di parametri al client

- Fase 2 – negoziazione SA

IKE: fasi

Le diverse modalità con cui si svolge la fase 1 dipendono solo dalla quantità di pacchetti usati per scambiarsi le informazioni.

Normalmente, il mittente invia una richiesta con parametri proposti, il destinatario risponde con quelli che accetta, poi si scambiano le chiavi ed il resto è criptato

Nella modalità più veloce, si usano 3 pacchetti in tutto, invece di 6. Il procedimento è più veloce, ma alcuni dati passano non criptati

IKE: funzionamento

- IKE usa per la prima fase l'algoritmo di scambio delle chiavi Diffie-Hellmann
- Si tratta di un sistema a chiave pubblica
- Crea un canale sicuro, per lo scambio della chiave utilizzata dalla funzione di hash

IKE: funzionamento

- Ognuno dei peer invia all'altro un numero generato opportunamente

- Entrambi concordano su uno dei due numeri, e da esso generano una chiave pubblica, spedita all'altro

- Per il meccanismo con cui funziona l'algoritmo, le due chiavi:

$$Pub(Pra) = Pua(Prb)$$

sono uguali e possono essere usate come chiave condivisa

IKE: proprietà

- IKE permette la rilevazione dei peer down (DPD), bidirezionale e periodica

- Visto che ESP cripta tutto il contenuto L4, compresa la porta, la presenza di NAT/PAT sul percorso rende necessario il NAT Trasversal, mediante l'aggiunta di un wrapper UDP

- La presenza del NAT e l'eventuale uso del NAT Trasversal sono decisi in Fase 1 ed in Fase 2

ESP e AH

- ESP (protocollo 50) inserisce un header e cripta il contenuto del pacchetto. In particolare copre il payload del pacchetto.

- Si può usare anche per autenticazione

- AH (protocollo 51) non fornisce criptazione dei dati, ma aggiunge un pacchetto di informazione che permette di verificare l'integrità del contenuto

- Non permette di garantire la riservatezza

Modalità Tunnel

- Tunnel Mode – questa modalità incapsula tutto il pacchetto IP. Vengono quindi generati nuovi header IP per permettere al pacchetto di proseguire il percorso

- Si può usare sia con ESP che con AH, e provoca un aumento delle dimensioni del pacchetto di 20 byte

- E' possibile configurare sugli apparati gli IP che vengono assegnati ai pacchetti per il passaggio

Modalità Transport

- Transport Mode – il Tunnel Mode è oneroso per pacchetti piccoli. Questa modalità inserisce il suo header ESP fra l'IP ed il contenuto di livello superiore (es. TCP)

- Più piccolo, ma espone gli indirizzi della comunicazione (IP) alla rilevazione

- Solitamente si usa insieme al protocollo GRE, che aggiunge un suo header IP

Modalità Tunnel e Transport (2)

- Il Transport Mode lascia esposti gli header IP originali, perché sono usati per il routing

- Se si usa Tunnel Mode, di solito sono i gateway che terminano la rete “verso Internet”, che si occupano di aggiungere ed eliminare gli header IP che servono per il trasporto

- Questo secondo metodo è quindi più sicuro, perché gli unici indirizzi esposti sono quelli dei gateway

ESP e AH: header

- AH genera un hash, che attacca al pacchetto originario, garantendo autenticità ed integrità.

- ESP cripta il pacchetto originale, ed eventualmente setta un bit per evitare le rispedizioni.

- ESP può essere usato insieme ad un algoritmo AH, che crea un hash dal pacchetto criptato

- Sono così garantiti confidenzialità, autenticazione, integrità

AH, funzionamento

- Il contenuto del pacchetto iniziale viene usato per generare l'hash
- L'header AH è inserito fra header IP e payload
- Il ricevente prende header IP e payload, calcola l'hash
- Se corrisponde a quello nell'header AH, passa il pacchetto IP, altrimenti lo scarta
- Non c'è criptazione

ESP, funzionamento

- Il contenuto del pacchetto iniziale viene criptato ed incapsulato da un header ed un trailer ESP
- Tutto il pacchetto ora ottenuto viene sottoposto ad hash
- Si aggiunge un header IP nuovo, che permetta di arrivare a destinazione
- Il primo controllo è quello dell'hash. Se fallisce, non c'è bisogno di decriptare e si scarta il pacchetto

Controllo autenticazione

- La porzione di servizio dedicata, negli apparati CISCO, al controllo dell'autenticazione e dell'integrità è detto HMAC

- Si basa su funzioni come MD5 o SHA-1, che determinano la robustezza complessiva dell'algoritmo

- In questo caso al messaggio vero e proprio viene aggiunta una chiave per la generazione dell'hash, richiesta anche in fase di verifica

VPN - funzionamento

- Una situazione tipica è quella di una VPN fra due sedi remote.
- Le reti delle sedi accedono a Internet attraverso router
- Il procedimento si divide in pratica in 5 fasi

VPN – le 5 fasi

1. Il traffico che deve essere criptato è intercettato mediante access-list sull'interfaccia ed attiva il collegamento IPsec

2. IKE, fase 1 – creazione del canale sicuro per la fase 2

3. IKE, fase 2 – negoziazione dei parametri di sicurezza per il trasferimento dati

4. Trasferimento dati (criptati)

5. Chiusura della connessione

VPN – scelta traffico

- Il traffico in uscita dal router viene controllato da ACL presenti sulle diverse interfacce
- Se ricade nella ACL del tunnel criptato, viene attivato il processo relativo
- Sono possibili anche diversi schemi di criptazione per diverse categorie di traffico
- Lo stesso principio si usa nei PC con client VPN

VPN – IKE fase 1

- Come già visto, in questa fase i due router devono accordarsi sugli algoritmi di hash e di criptazione
- Ogni router possiede dei “transform set”, combinazioni di valori diversi dei parametri di sicurezza
- Si scambiano le proprie informazioni e usano il primo set su cui “concordano”
- Questo è molto comodo se i peer remoti sono diversi

VPN – IKE fase 1

- La fase di scambio delle chiavi può comportare due diversi "gruppi", a cui corrispondono lunghezze diverse dei numeri usati per la generazione delle chiavi (768 o 1024)

- Dopo la generazione della chiave condivisa, è necessario autenticare il peer remoto

- Questo avviene mediante: chiave condivisa preventivamente, firma RSA o numeri casuali scambiati sempre con algoritmo RSA

VPN – IKE fase 2

- Negoziazione dei parametri per la SA della fase IPsec
- Definizione della SA IPsec e cambio periodico dei parametri
- Anche in questo caso si utilizzano transform set, il primo su cui i due router concordano contiene gli algoritmi che formano la SA
- Le informazioni sulle SA vengono registrate in due db (SPD e SAD) con cui decidere come operare sul traffico in ingresso o in uscita

VPN – trasferimento

- Il traffico passa nel canale sicuro, definito dalle SA (una per ogni flusso)
- Il trattamento sui due peer dipende dai db che contengono i parametri
- E' possibile scambiare anche ulteriori parametri SA, quando termina il tempo di vita di quelle dei collegamenti precedenti
- Per ogni sessione vengono negoziati nuovi parametri

VPN – chiusura

- Il tunnel criptato viene chiuso
  - Dal timeout di una delle SA
  - Dal contatore di pacchetti
- Le chiavi vengono distrutte, per continuare a scambiare dati è necessaria una nuova fase 2 (ed eventualmente una fase 1)
- Di solito i parametri per la nuova fase 2 sono scambiati prima della fine della precedente, in modo da avere flusso continuo

Agenda

- Cosa è il CINECA
- Accesso remoto e Crittografia
- VPN IPsec
- Esempi di configurazione
  - Site to Site
  - via client

VPN – Configurazione

La configurazione di una VPN site-to-site comprende:

1. Definire una policy ISAKMP (per il tunnel IKE)
2. Configurare i transform set IPsec (per il tunnel IPsec)
3. Configurare le crypto ACL (quale traffico viene criptato)
4. Configurare le crypto map (raggruppa i parametri precedenti)
5. Applicare le crypto map all'interfaccia (di uscita)
6. Configurare le ACL sulle interfacce (per protezione, di solito blocca tutto il traffico non IPsec o IKE)

VPN – Configurazione (1)

```
crypto isakmp policy 20
 encr aes
 authentication pre-share
 group 2
 lifetime 3600
!
crypto isakmp policy 30
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp policy 40
 encr 3des
 hash md5
 authentication pre-share
```

- Definizione dei parametri per lo scambio delle chiavi
- Un apparato può avere diversi set di parametri
- Il peer con cui si comunica deve avere un set di parametri compatibile o uguale, anche con numero di policy diverso

VPN – Configurazione (1)

```
crypto isakmp key 6 QJZVEGLVXD]P[gRbWHadOBU_YU\BZgPdh^BY`aieHGAAB
address <IP PEER 1> no-xauth
crypto isakmp key 6 O[`ePSfBYXfCVfVMYU\`XZC`\PCBNGEXGSX` address <IP
PEER 2>
crypto isakmp key 6 [CLW\FWMd\YSf^SOShYai\ggffebU_AN_XWSFVO]bFAAB
address <IP PEER 3> no-xauth
crypto isakmp keepalive 10
crypto isakmp xauth timeout 30
```

- Definizione delle chiavi per le comunicazioni con i diversi peer
- Nella configurazione dell'apparato risultano criptate
- Anche in questo caso, l'interlocutore deve usare la stessa chiave

VPN – Configurazione (2-5)

- Definizione del/dei transform set
- Definizione della ACL che identifica il traffico da criptare
- Definizione di una crypto map, che associa i parametri precedenti ed eventualmente il peer
- Questa crypto map viene poi associata ad una interfaccia fisica

VPN – Configurazione (2)

```
crypto ipsec transform-set 3des-sha esp-3des esp-sha-hmac
crypto ipsec transform-set 3des-md5 esp-3des esp-md5-hmac
crypto ipsec transform-set des-sha-hmac esp-des esp-sha-hmac
crypto ipsec transform-set 3des-sha-hmac esp-3des esp-sha-hmac
crypto ipsec transform-set des-md5-hmac esp-des esp-md5-hmac
crypto ipsec transform-set 3des-md5-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set aes-sha-hmac esp-aes 256 esp-sha-hmac
```

- I diversi set di algoritmi individuano le combinazioni che si useranno per lo scambio IPsec

VPN – Configurazione (3)

```
ip access-list extended vpn-Cineca-CUSTOMER1
 permit ip 10.254.8.16 0.0.0.7 host <IP REMOTE HOST>
 permit ip 10.254.8.16 0.0.0.7 <IP REMOTE NETWORK>
 permit ip host 10.254.8.24 host <IP REMOTE HOST>
 permit ip host 10.254.8.24 <IP REMOTE NETWORK>
```

- La ACL contiene un permit per il traffico diretto verso la VPN (in questo caso quello dalle reti indicate all'host remoto
- La destinazione può essere un host, una rete o più elementi
- L'ACL sull'altro peer deve essere simmetrica, ma identica, compreso il numero di righe (non possono essere raggruppate diversamente)
- Nell'esempio l'ACL è di tipo esteso, ma non è obbligatorio

VPN – Configurazione (3)

```
ip access-list extended policy-CUSTOMER2
 permit ip host 130.186.XX.YY <NETWORK1>
 permit ip host 130.186.XX.YY <NETWORK2>
 permit ip host 130.186.XX.YY <NETWORK3>
```

- Questo è un caso identico al precedente, che serve però ad esemplificare un ulteriore passo di configurazione

VPN – Configurazione (4)

```
crypto map vpn-outside 50 ipsec-
isakmp
 set peer <IP PEER CUSTOMER1>
 set transform-set 3des-md5-hmac
 match address vpn-Cineca-
CUSTOMER1
crypto map vpn-outside 60 ipsec-
isakmp
 set peer <IP PEER CUSTOMER2>
 set transform-set aes-sha-hmac
 match address vpn-Cineca-
CUSTOMER2
…
route-map CUSTOMER2 permit 10
 match ip address policy-
CUSTOMER2
 set interface GigabitEthernet0/0
```

- Nella prima riga c'è il nome della crypto map, ed un numero che identifica diversi gruppi di regole
- Quando il traffico corrisponde alle righe di ACL indicate, si attiva la connessione IPsec
- La connessione avviene con il peer ed il set di parametri indicati

VPN – Configurazione (5)

```
interface GigabitEthernet0/0
 description VPN-OUTSIDE
 ip address 193.204.120.198
255.255.255.240
…
 ip policy route-map CUSTOMER2
…
 crypto map vpn-outside
```

- All'interfaccia è applicata la crypto map definita al punto precedente
- Queste contengono già le indicazioni sul traffico da instradare e le modalità relative
- L'istruzione sul policy routing permette di forzare del traffico sulla base di un criterio più specifico (es. quando ci sono sovrapposizioni di indirizzi privati)

Agenda

- Cosa è il CINECA
- Accesso remoto e Crittografia
- VPN IPsec
- Esempi di configurazione
  - Site to Site
  - via client

VPN – Configurazione Client (1)

```
crypto isakmp client configuration group
vpn-CLIENT
 key 6 <chiave criptata>
 <indirizzi DNS e WINS>
 pool CLIENT
 acl vpn-CLIENT

ip local pool CLIENT 192.168.82.1
192.168.82.254
ip nat inside source list 103 pool
NATCLIENT overload
access-list 103 permit ip 192.168.82.0
0.0.0.255 any
ip nat pool NATCLIENT 130.186.8.184
130.186.8.190 prefix-length 29
```

- Per i client, ci sono delle definizioni aggiuntive
- Quando il client si connette, scambia la chiave presente nella configurazione
- L'indirizzo assegnato viene da un pool assegnato
- Si definiscono anche le regole con cui verranno nattati tali indirizzi

VPN – Configurazione Client (2)

```
ip access-list extended vpn-CLIENT
 permit ip host <IPHOST> <NETWORK CLIENT>
 permit ip <NETWORK DEST.> <NETWORK
CLIENT>

crypto ipsec profile VPNCLIENT
 set transform-set 3des-sha
 set isakmp-profile VPNCLIENT

crypto isakmp profile VPNCLIENT
   match identity group vpn-CLIENT
   client authentication list VPN
   isakmp authorization list VPNGROUP
   …
   virtual-template 5
```

- L'ACL serve come al solito per individuare il traffico
- Il profilo IPsec contiene le informazioni per criptare il traffico
- L'autenticazione, in questo caso, è fatta tramite un server Radius

VPN – Configurazione Client (3)

```
interface Virtual-Template5 type tunnel
 ip unnumbered Loopback0
 ip nat inside
 ip virtual-reassembly
 ip policy route-map VPNDINAMIC
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
VPNCLIENT

route-map VPNDINAMIC permit 10
 match ip address policy
 set ip next-hop 192.168.77.1
```

- L'applicazione all'interfaccia riassume tutto
- Viene applicato il NAT
- Il traffico da proteggere è individuato dal profilo IPsec
- Il policy routing è quasi sempre necessario, in questo caso instrada il traffico verso il firewall

Riferimenti

Ing. Vincenzo Vaccarino

CINECA
Dipartimento Sistemi e Tecnologie
Settore Operazioni

Tel. 051/6171411 (centralino)
Email: v.vaccarino@cineca.it