D.Lgs.196/2003

Come proteggere la propria stazione di lavoro

Gaetano Pisano

Centro Universitario di Calcolo

Università degli Studi di Palermo

Stazione di lavoro collegata alla rete dati di Ateneo

Una stazione di lavoro collegata alla rete dati di Ateneo deve avere associato un indirizzo IP (Internet Protocol) né più e né meno di come un qualsiasi telefono, collegato alla rete di telefonica, deve avere associato un numero telefonico.

Così come tutti i numeri telefonici che insistono nell'area di Palermo cominciano con il prefisso "091", gli indirizzi IP della Università degli Studi di Palermo cominciano con "147.163."; il terzo numero tipicamente indica la struttura di appartenenza (es. la rete del CUC è identificata col terzo numero pari a "1") e il quarto numero identifica la stazione di lavoro nella rete (es. 147.163.1.5 è l'indirizzo IP associato al sito web www.unipa.it)

%

Ogni trasmissione dati, così come una qualsivoglia chiamata telefonica,è dunque caratterizzata da due attori con due indirizzi IP distinti, uno che si chiama (client) e l’altro che risponde ed eroga servizi (server).

Porte TCP e UDP

I Computer sono in grado di svolgere più operazioni nell'unità di tempo e, nella fattispecie, un computer con funzioni di server può rispondere contemporaneamente a più "client"; per distinguere le varie trasmissioni di dati che si possono instaurare oltre agli indirizzi IP, che identificano i computer, entrano in gioco le "porte" TCP (Transmission Control Protocol) e UDP (User Datagram Protocol), che identificano i "servizi"; le porte più comuni, lato server, sono:

Web, porta TCP 80

Proxy, porta TCP 3128

Posta elettronica in uscita, porta TCP 25

Posta elettronica in entrata, porta TCP 110 (POP) e porta TCP 143 (IMAP)

....

I client invece, per ogni connessione, utilizzano una porta con numero compreso tra 1024 e 65535.

Il ruolo del DNS

- Si capisce bene come possa essere difficile ricordare a memoria gli indirizzi IP dei server con i quali normalmente si lavora; per facilitare l'associazione tra indirizzo IP e nome mnemonico interviene il server DNS (Domain Name Server) che traduce i cosiddetti nomi a dominio Internet (es. www.unipa.it) nel relativo indirizzo IP (es. 147.163.1.5)
- I server DNS di Ateneo hanno indirizzo IP 147.163.1.22 e 147.163.1.3

Il ruolo del WINS

- Ogni PC con sistema operativo Windows ha un nome e appartiene a un gruppo di lavoro. Per avere un elenco aggiornato delle informazioni: “nome”, “gruppo di lavoro” e “indirizzo IP” occorre riferirsi ad un WINS (Windows Internet Name Server) server;
- Il server WINS di Ateneo ha indirizzo IP 147.163.1.49

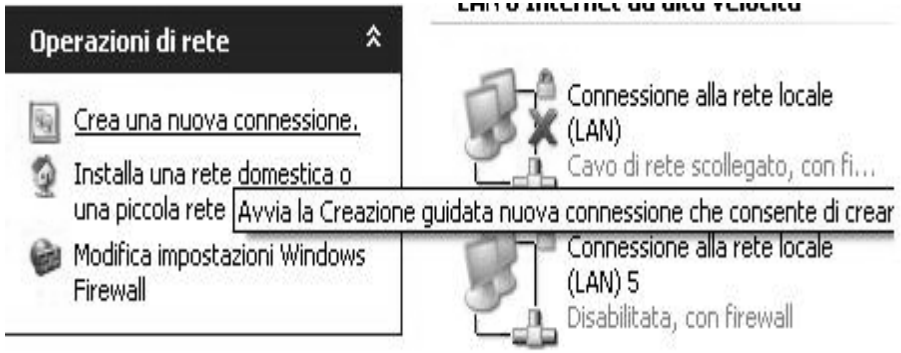
Il VPN server

Una VPN è letteralmente un Virtual Private Network: significa che, tramite un VPN server, se ci trova a casa, connessi in ADSL con un qualsiasi fornitore di connettività (Telecom, Infostrada, …) si può stabilire una connessione tale da far funzionare la propria stazione di lavoro nell'ambito in cui è fisicamente attivo il VPN server.

In breve, se sono un incaricato relativo alla contabilità e voglio operare da casa tramite una connessione ADSL, posso farlo purchè sia collegato con il VPN server del CUC che risponde all'indirizzo IP 147.163.1.88

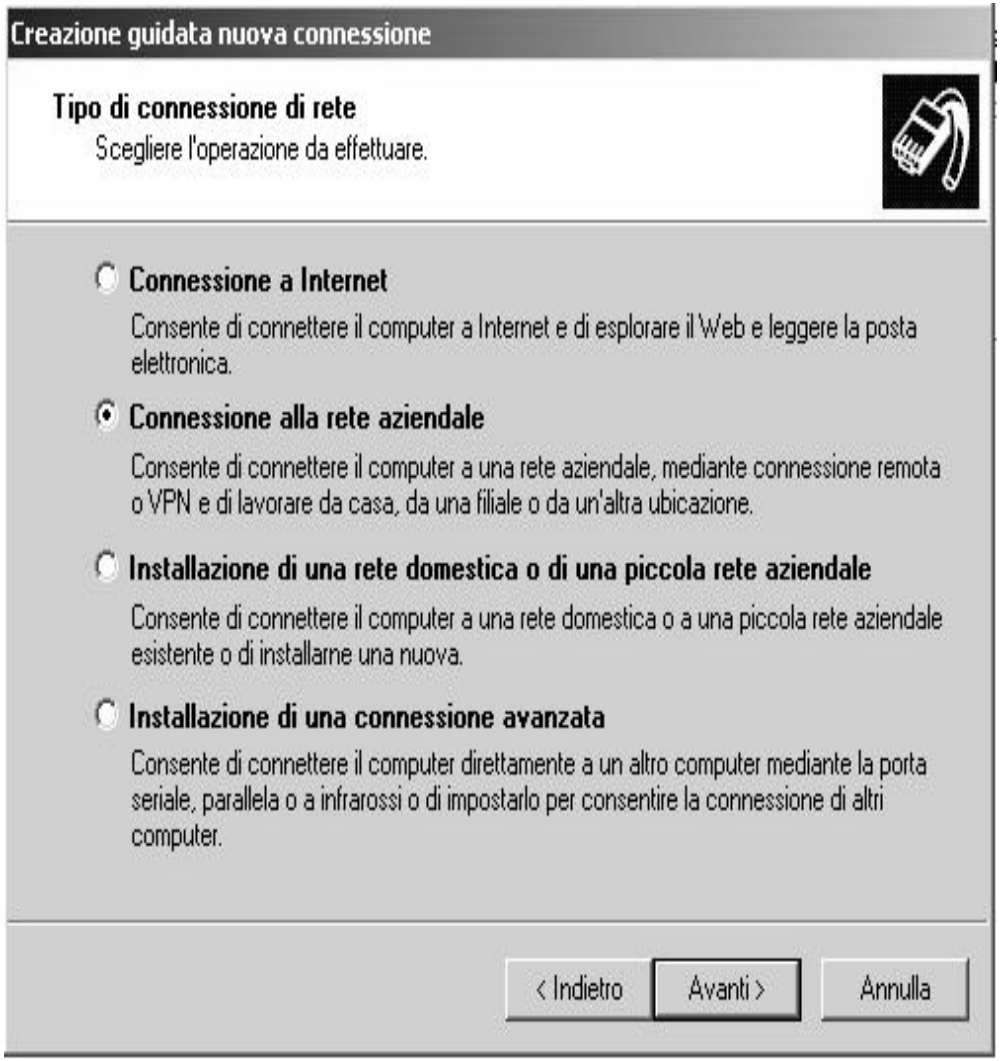
%


Risorse di
Apri
Esplora
Cerca computer...
Connetti unità di rete...
Disconnetti unità di rete...
Crea collegamento
Elimina
Rinomina
Proprietà

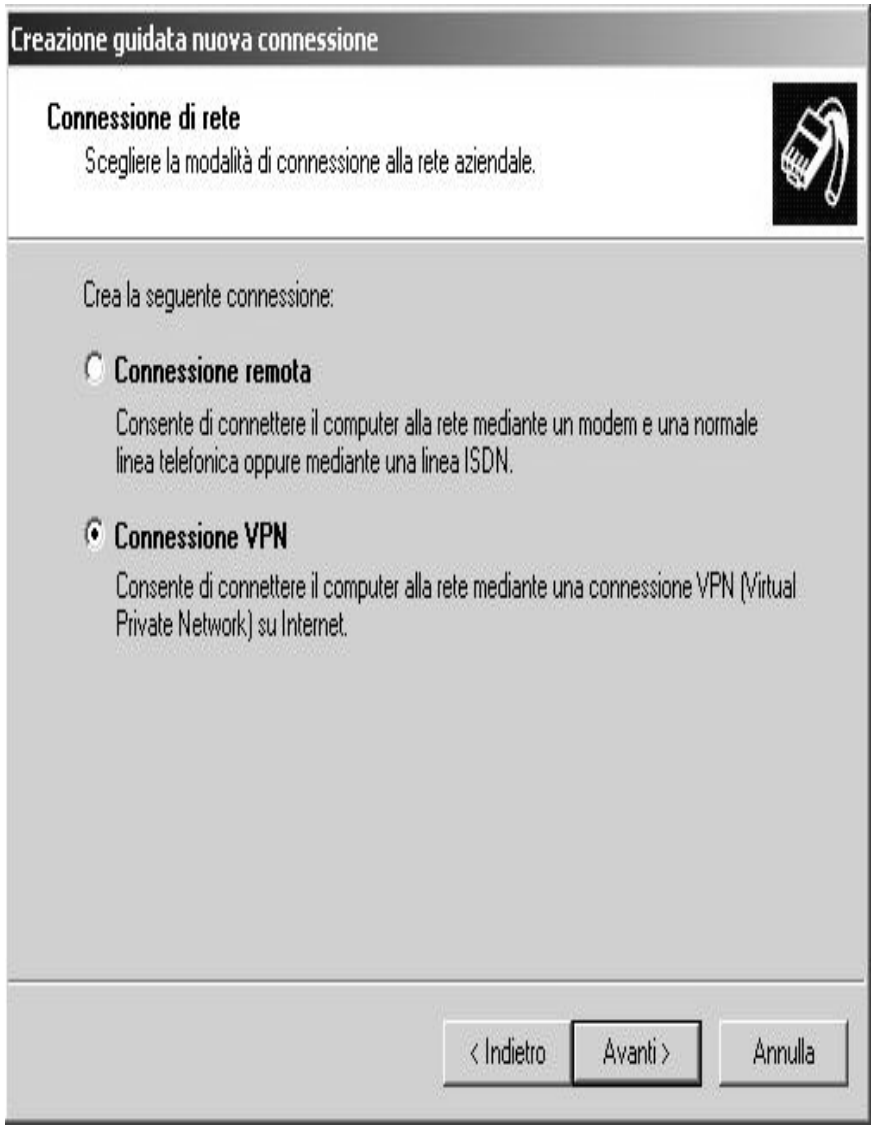

Operazioni di rete
Crea una nuova connessione.
Installa una rete domestica o una piccola rete
Modifica impostazioni Windows Firewall
Connessione alla rete locale (LAN)
Cavo di rete scollegato, con fi...
Avvia la Creazione guidata nuova connessione che consente di crear
Connessione alla rete locale (LAN) 5
Disabilitata, con firewall

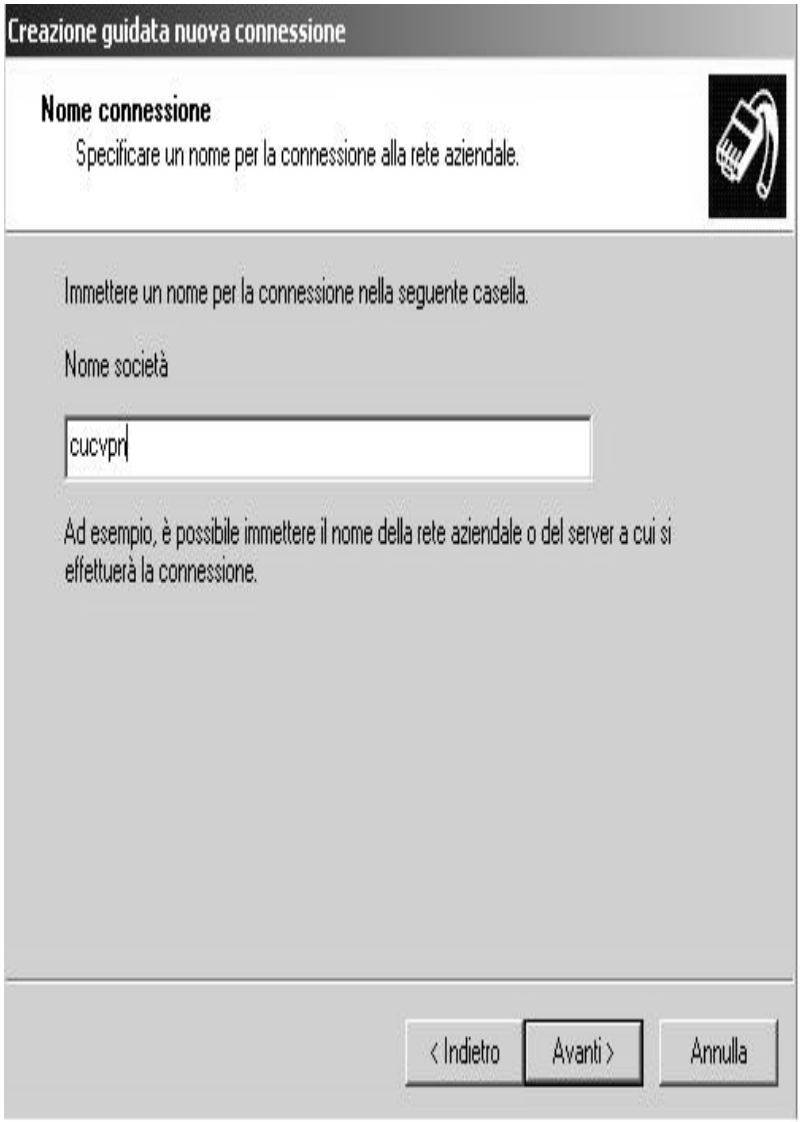
%


Creazione guidata nuova connessione
Creazione guidata nuova connessione
Questa procedura guidata consente di:
• Connettere il computer a Internet.
• Connettere il computer a una rete privata, come una rete aziendale.
• Installare una rete domestica o una piccola rete aziendale.
Per continuare, scegliere Avanti.
< Indietro
Avanti >
Annulla

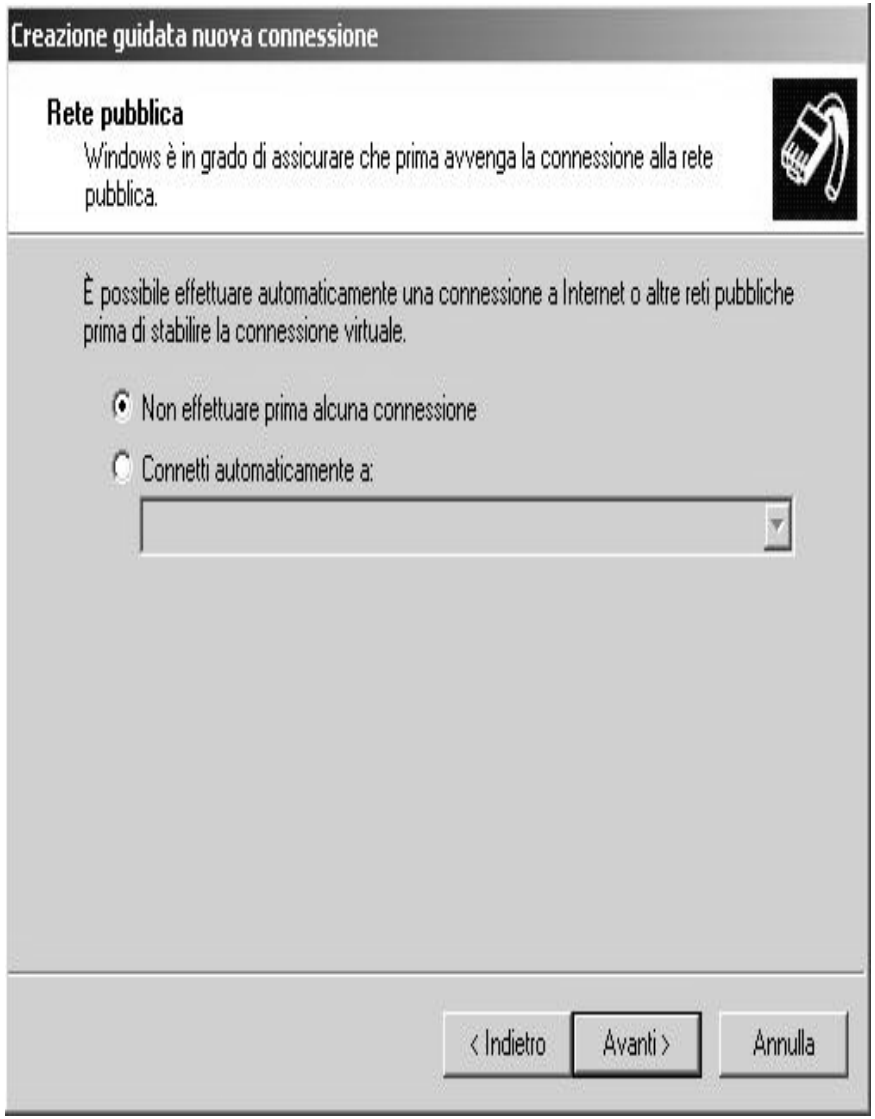

Creazione guidata nuova connessione
Tipo di connessione di rete
Scegliere l'operazione da effettuare.
Connessione a Internet
Consente di connettere il computer a Internet e di esplorare il Web e leggere la posta elettronica.
Connessione alla rete aziendale
Consente di connettere il computer a una rete aziendale, mediante connessione remota o VPN e di lavorare da casa, da una filiale o da un'altra ubicazione.
Installazione di una rete domestica o di una piccola rete aziendale
Consente di connettere il computer a una rete domestica o a una piccola rete aziendale esistente o di installarne una nuova.
Installazione di una connessione avanzata
Consente di connettere il computer direttamente a un altro computer mediante la porta seriale, parallela o a infrarossi o di impostarlo per consentire la connessione di altri computer.
< Indietro
Avanti >
Annulla

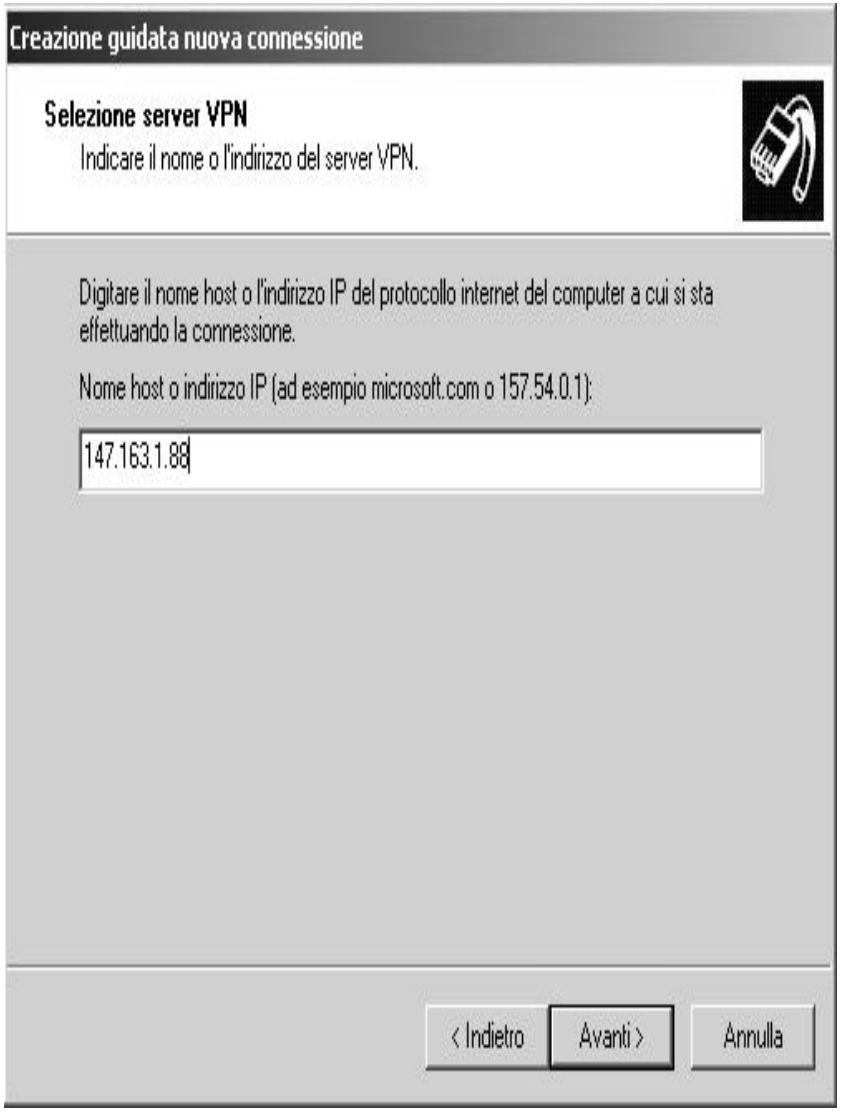
%


Creazione guidata nuova connessione
Connessione di rete
Scegliere la modalità di connessione alla rete aziendale.
Crea la seguente connessione:
Connessione remota
Consente di connettere il computer alla rete mediante un modem e una normale linea telefonica oppure mediante una linea ISDN.
Connessione VPN
Consente di connettere il computer alla rete mediante una connessione VPN (Virtual Private Network) su Internet.
< Indietro
Avanti >
Annulla

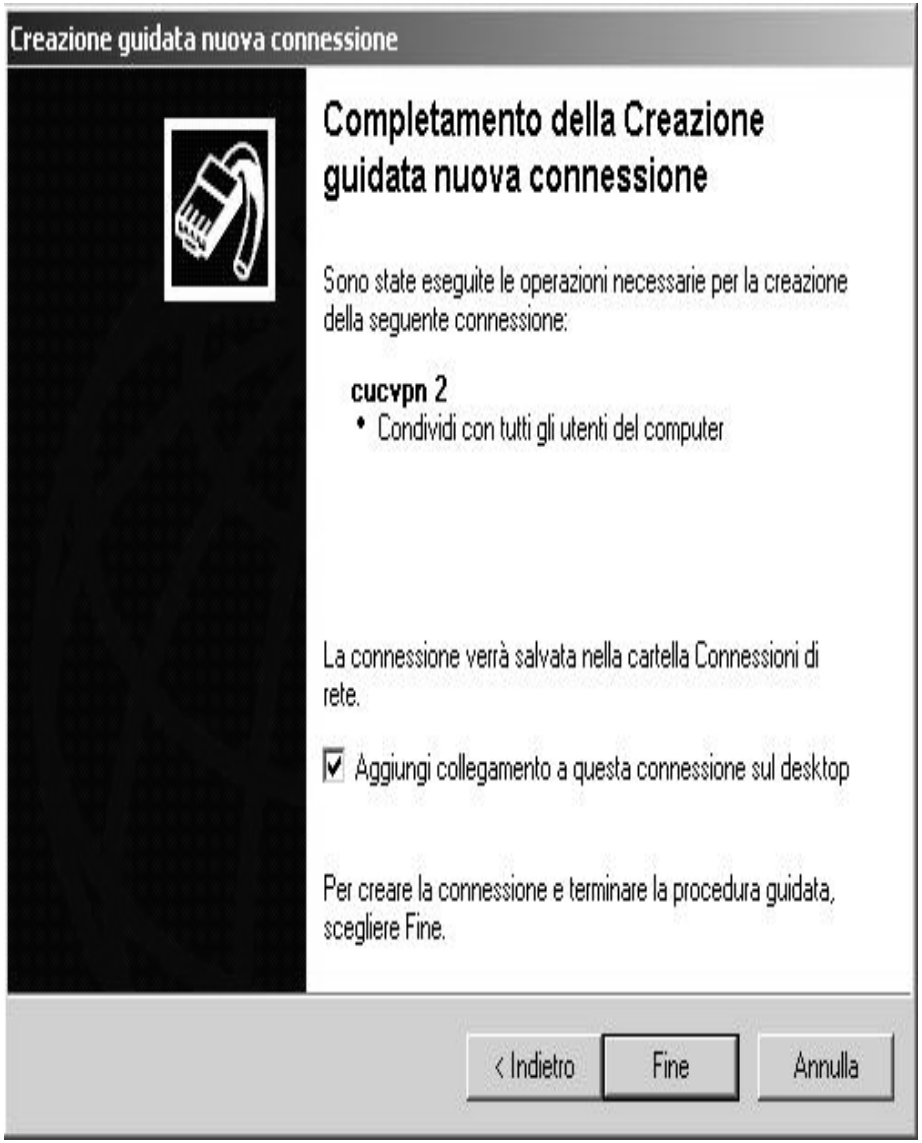

Creazione guidata nuova connessione
Nome connessione
Specificare un nome per la connessione alla rete aziendale.
Immettere un nome per la connessione nella seguente casella.
Nome società
cucvpn
Ad esempio, è possibile immettere il nome della rete aziendale o del server a cui si effettuerà la connessione.
< Indietro
Avanti >
Annulla

%


Creazione guidata nuova connessione
Rete pubblica
Windows è in grado di assicurare che prima avvenga la connessione alla rete pubblica.
È possibile effettuare automaticamente una connessione a Internet o altre reti pubbliche prima di stabilire la connessione virtuale.
Non effettuare prima alcuna connessione
Connetti automaticamente a:
< Indietro
Avanti >
Annulla


Creazione guidata nuova connessione
Selezione server VPN
Indicare il nome o l'indirizzo del server VPN.
Digitare il nome host o l'indirizzo IP del protocollo internet del computer a cui si sta effettuando la connessione.
Nome host o indirizzo IP (ad esempio microsoft.com o 157.54.0.1):
147.163.1.88
< Indietro
Avanti >
Annulla

%


Creazione guidata nuova connessione
Completamento della Creazione guidata nuova connessione
Sono state eseguite le operazioni necessarie per la creazione della seguente connessione:
cucvpn 2
• Condividi con tutti gli utenti del computer
La connessione verrà salvata nella cartella Connessioni di rete.
Aggiungi collegamento a questa connessione sul desktop
Per creare la connessione e terminare la procedura guidata, scegliere Fine.
< Indietro
Fine
Annulla


Connessione a cucvpn
Nome utente:
pisano
Password:
[Per cambiare la password salvata, fare clic qui]
Salva nome utente e password per gli utenti seguenti:
Solo utente corrente
Qualsiasi utente
Connetti
Annulla
Proprietà
?

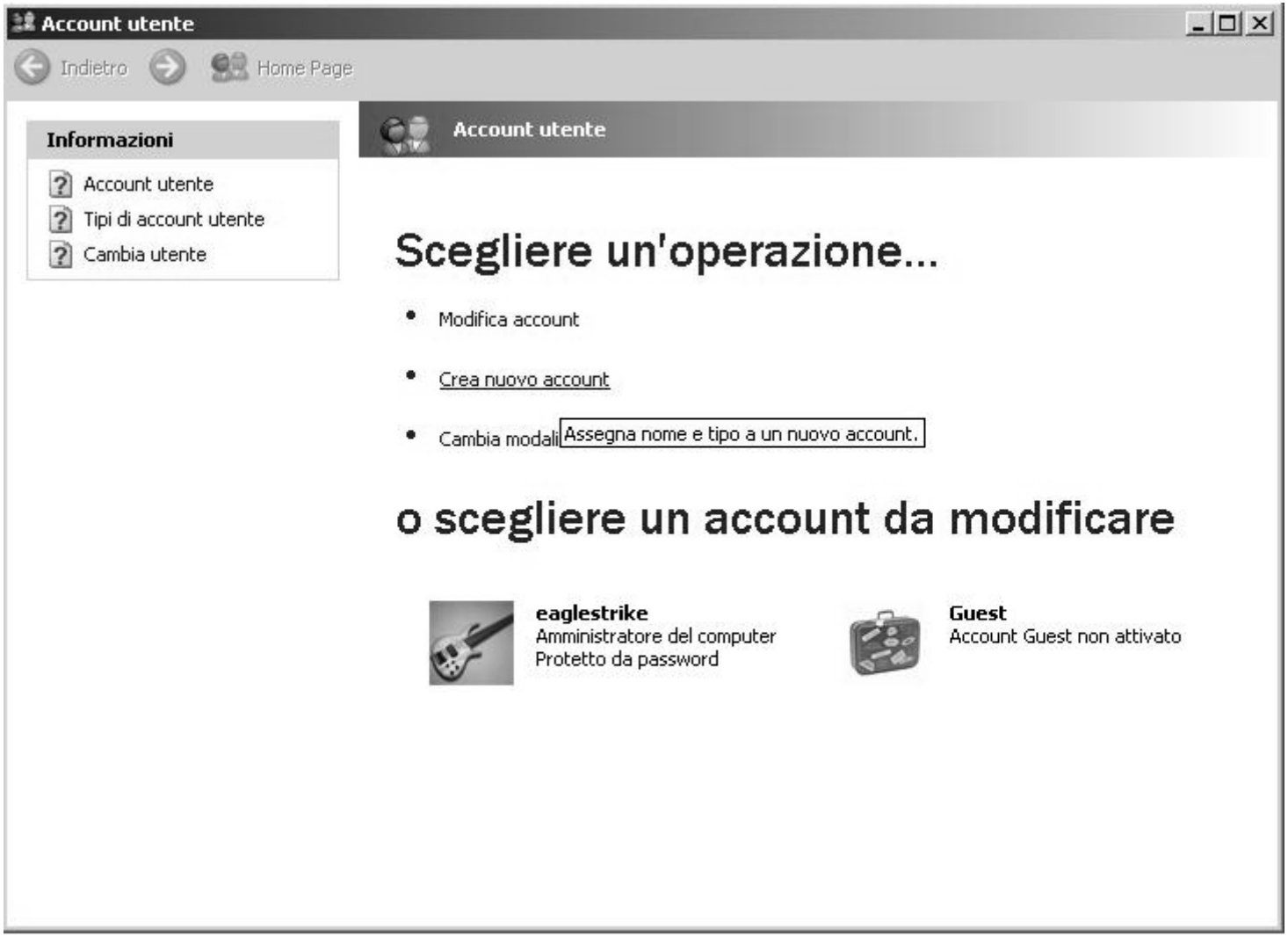
%

Creare Password di BIOS

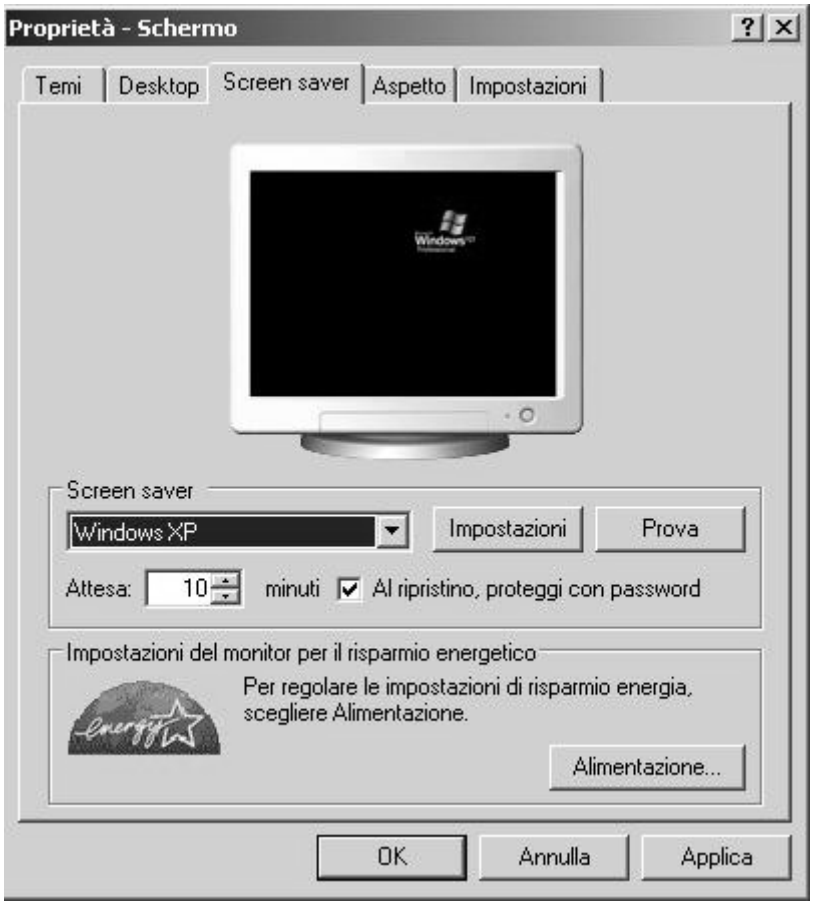
Creare nuovo utente in WinXp

1. Nella casella di riepilogo **Scegliere un'operazione** fare clic su **Crea nuovo account**.
2. Digitare il nome che si desidera utilizzare per l'account, quindi scegliere **Avanti**.
3. Fare clic su un tipo di account desiderato, quindi scegliere **Crea account**.

%


Account utente
Indietro
Home Page
Informazioni
Account utente
Tipi di account utente
Cambia utente
Account utente
Scegliere un'operazione...
Modifica account
Crea nuovo account
Cambia modali
Assegna nome e tipo a un nuovo account.
o scegliere un account da modificare
eaglestrike
Amministratore del computer
Protetto da password
Guest
Account Guest non attivato

Attivare salvaschermo

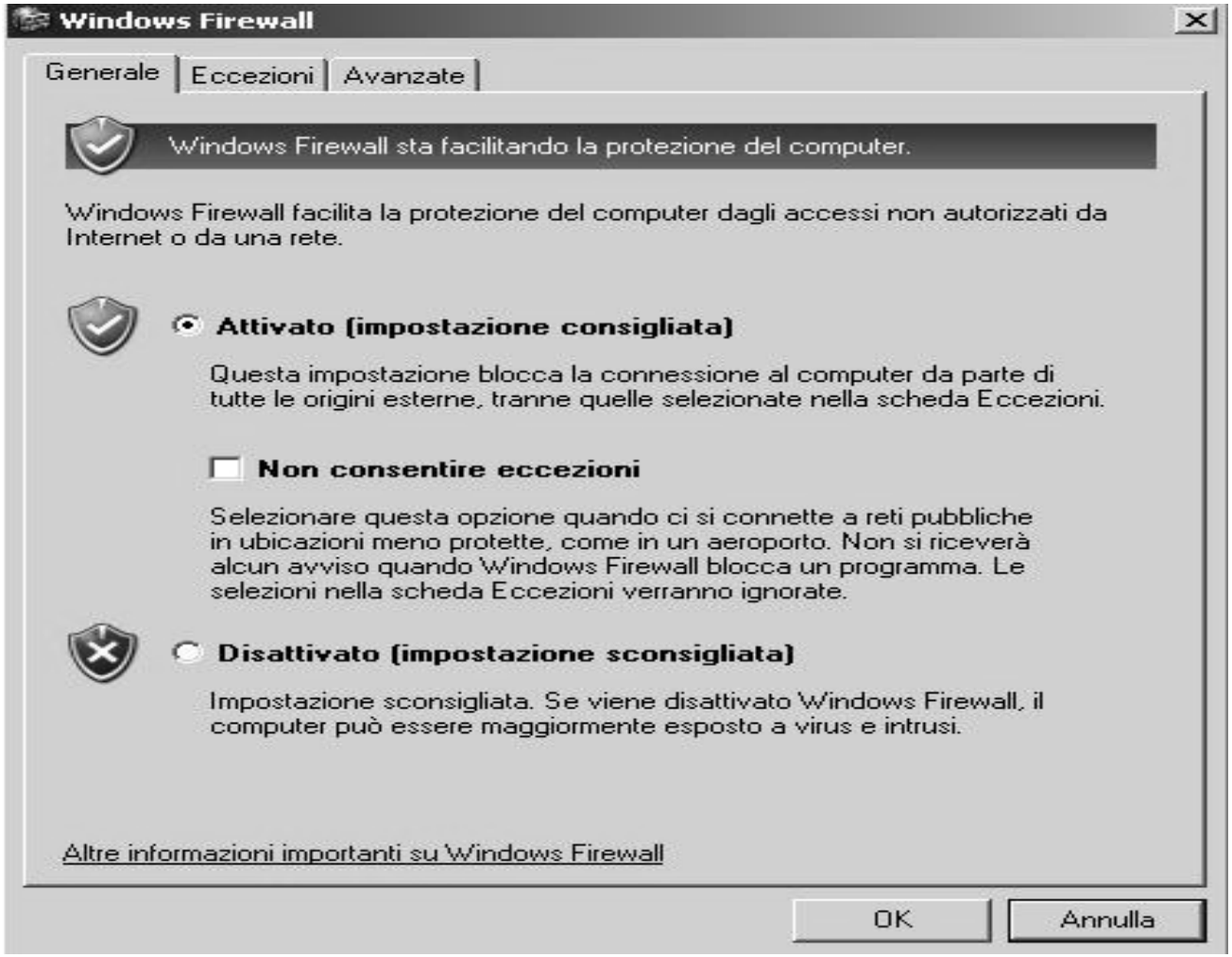


Firewall della stazione di lavoro

Funzione realizzata via software tale che controlla i dati trasmessi/ricevuti verso/da un computer e applica delle regole che contribuiscono alla sicurezza della stazione di lavoro.

%

Es. di firewall su Windows XP



%

Firewall perimetrale

Oltre al firewall che protegge la singola stazione di lavoro esistono anche i firewall che proteggono una intera rete locale e si chiamano firewall a protezione perimetrale.

I firewall perimetrali dell'Università degli Studi di Palermo applicano le regole di protezione su tutto il traffico dati, sia in entrata che in uscita verso e da Internet; per esempio, non si vuole che il server web www.unipa.it sia raggiungibile da Internet: si chiude sul firewall la porta 80 relativa all'indirizzo 147.163.1.5 a tutti coloro che provengono da Internet; è chiaro che tutti gli operatori universitari possono continuare a consultare il sito web in quanto questa regola sul firewall non li riguarda.
Al CUC sono sempre in funzione due firewall

%

IDS

Il firewall è solo uno dei componenti di una strategia di sicurezza informatica in quanto le sue funzionalità “consentono” o “negano”. Per controllare attivamente il traffico dati servono gli IDS (Intrusion Detection System) i quali si accorgono del passaggio di worm, virus, malware, spam, trojan, etc. ed eventuali connessioni non lecite.

Al CUC è sempre in funzione un IDS.

Log Server

Tutte le apparecchiature informatiche sono in grado di scrivere una sorta di “giornale di bordo” in cui sono elencate tutte le operazioni svolte dall’appbarecchiatura stessa. È importante concentrare tutte queste informazioni contemporaneamente in un unico server, denominato Log server, in modo tale che nessuna informazione possa sfuggire a chi gestisce il “sistema di rete” nel suo complesso.

Al CUC è sempre in funzione un Log Server.

NTP

Affinché gli orologi delle varie stazioni di lavoro siano sincronizzati, occorre Riferirsi ad un server in grado di offrire la data e l'orario in modo preciso. Ciò ris molto importante perché gli eventi vengano registrati in modo corretto nei files di log.

In Italia l'Istituto Galileo Ferraris di Torino, che funziona da NTP (Network Time Protocol) server, risponde all'IP 193.204.114.223 (time.ien.it).

L'NTP server dell'Università degli Studi di Palermo e risponde all'IP 147.163.1.3 (time.unipa.it).

SWATCH

Il Simple WATCHER (SWATCH) utilizza tutte le registrazioni sul Log server e allerta gli amministratori di sistema su eventi anomali (attacchi, password errate, etc..) intraprendendo una determinata azione (ad esempio bloccando l'indirizzo IP dell'attaccante).

Proxy server

Un **proxy** è un software che si interpone tra un client ed un server inoltrando le richieste e le risposte dall'uno all'altro.

Il client inoltra normalmente la sua richiesta di connessione, il proxy la intercetta, si collega al server e inoltra la risposta al client.

Per utilizzare un proxy è possibile configurare il client in modo che si colleghi al proxy invece che al server, oppure definire un **proxy trasparente**; in questo caso, a seconda della configurazione, alcune connessioni (ad esempio quelle HTTP) vengono automaticamente indirizzate al proxy senza che sia necessario configurare un client (quindi l'impostazione rimane attiva anche cambiando client).

Il proxy server del CUC ha indirizzo IP 147.163.1.17 e risponde sulla porta TCP 3128

%

Immagine di una normale navigazione web

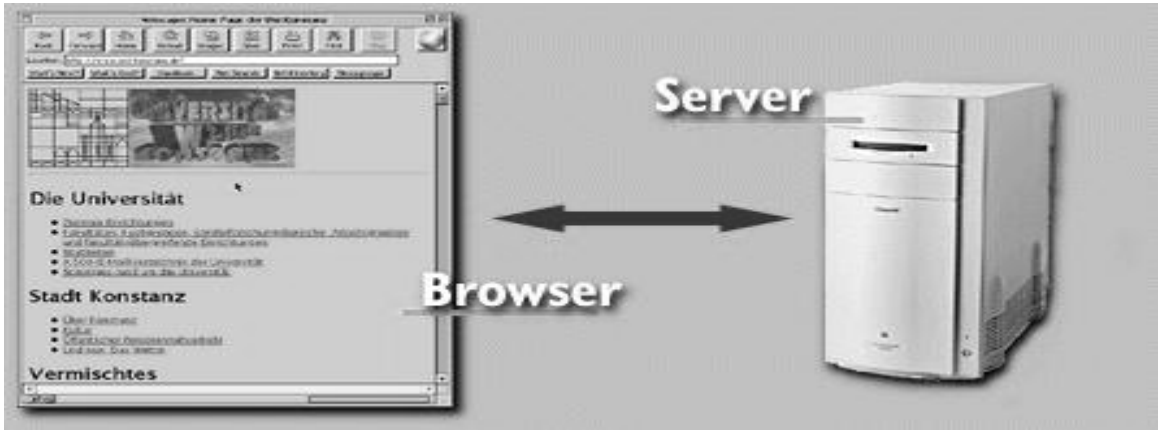
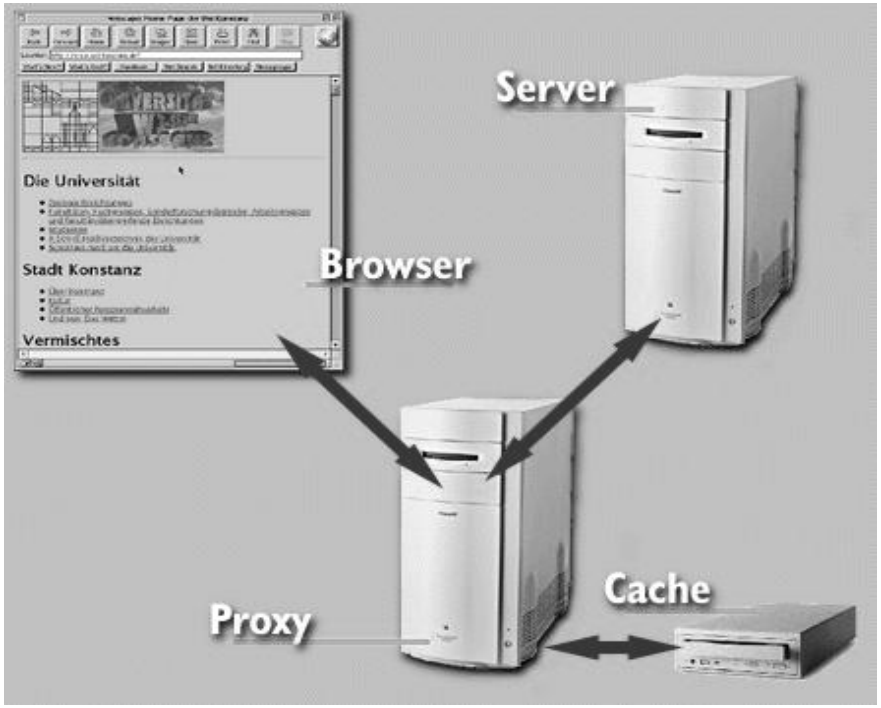


Immagine di una normale navigazione con proxy



%

Proxy server con content filtering e antivirus

Al proxy server è sempre utile associare un sistema di content filtering e antivirus.

DansGuardian è il sistema di *content filtering* adottato al CUC: si basa su una banca dati pubblica, denominata blacklist, e può essere personalizzata dall'amministratore di sistema in base alle esigenze di Ateneo.

Clamav è il sistema antivirus che protegge dalla eventualità di imbattersi in virus e troiani scaricati attraverso le pagine web.

%

L'ACCESSO E' STATO NEGATO -

L'accesso alla pagina:

http://big.dada.net

... e' stato negato per il seguente motivo:

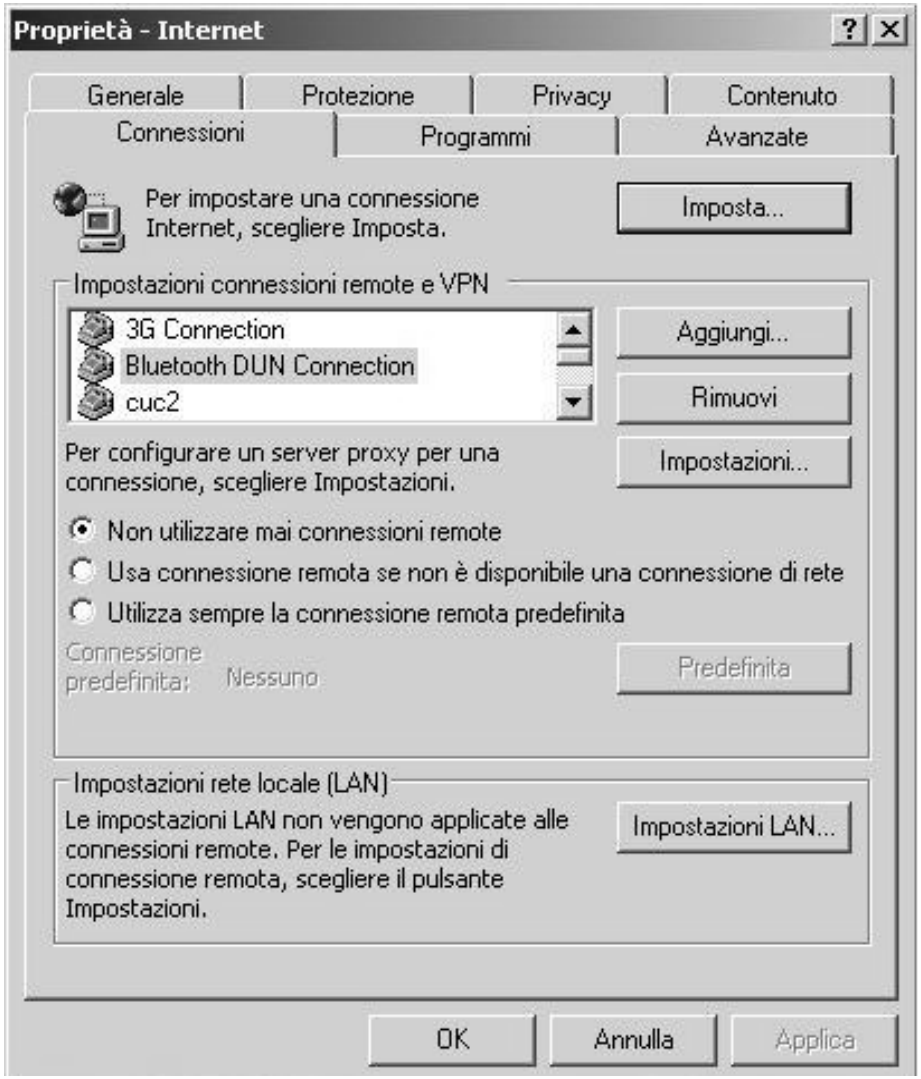
E' stato superato il limite per le frasi pesate.

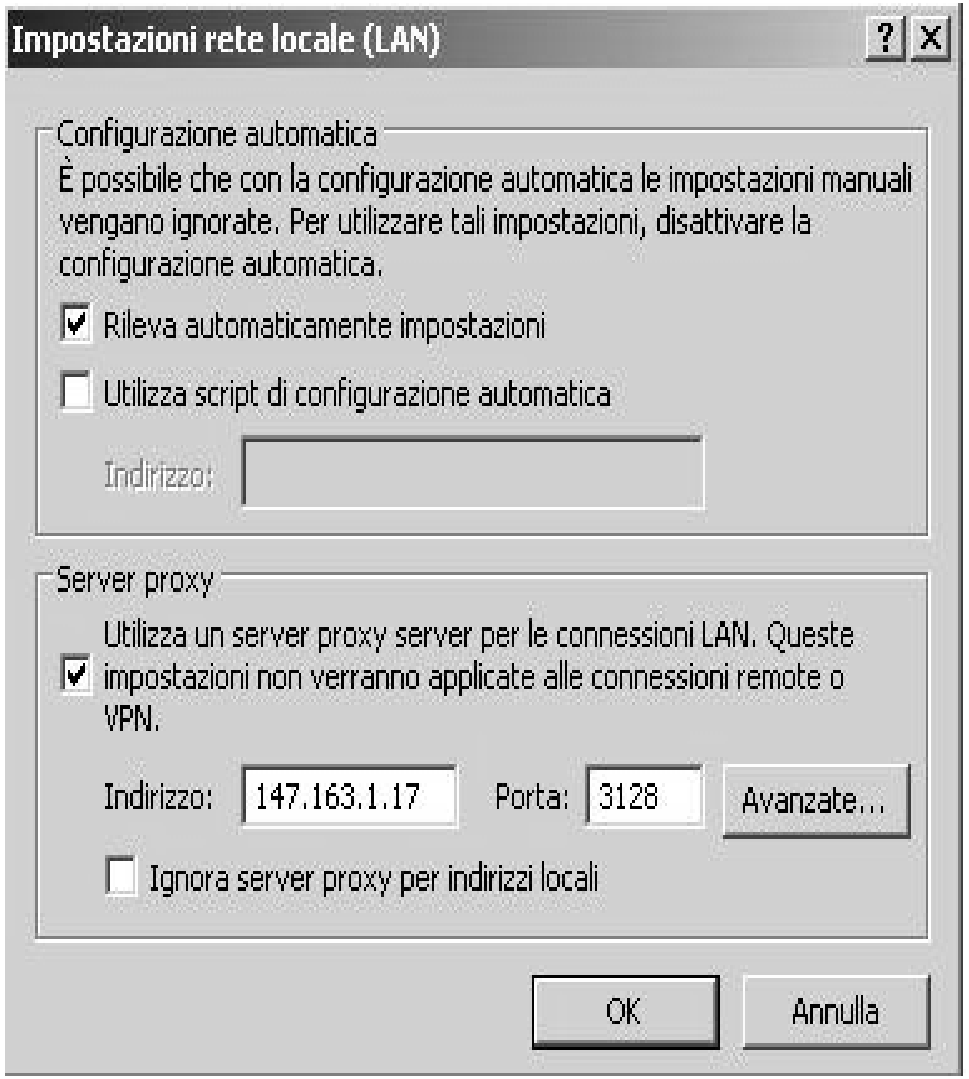
Stai vedendo questo errore perche' la pagina che hai cercato di accedere contiene, o e' marcata come contenente, materiale che e' stato ritenuto non appropriato.

Se hai ulteriori domande, contatta il tuo coordinatore ICT o Network Manager.

Powered by Dans Guardian

Per configurare il proxy server ..





%

Malware, parte I

•Virus: sono parti di programma che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti o via rete.

•Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di social engineering, oppure sfruttano dei difetti (bug) di alcuni programmi per diffondersi automaticamente.

•Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima.

%

Malware, parte II

Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso di emergenza ad un sistema.

Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

•Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo truffaldino, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

%

Malware, parte III

- Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattuto browser) e causano l'apertura automatica di pagine Web indesiderate.
- Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da delle copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in se ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare *spyware* e *trojan*.
- Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.

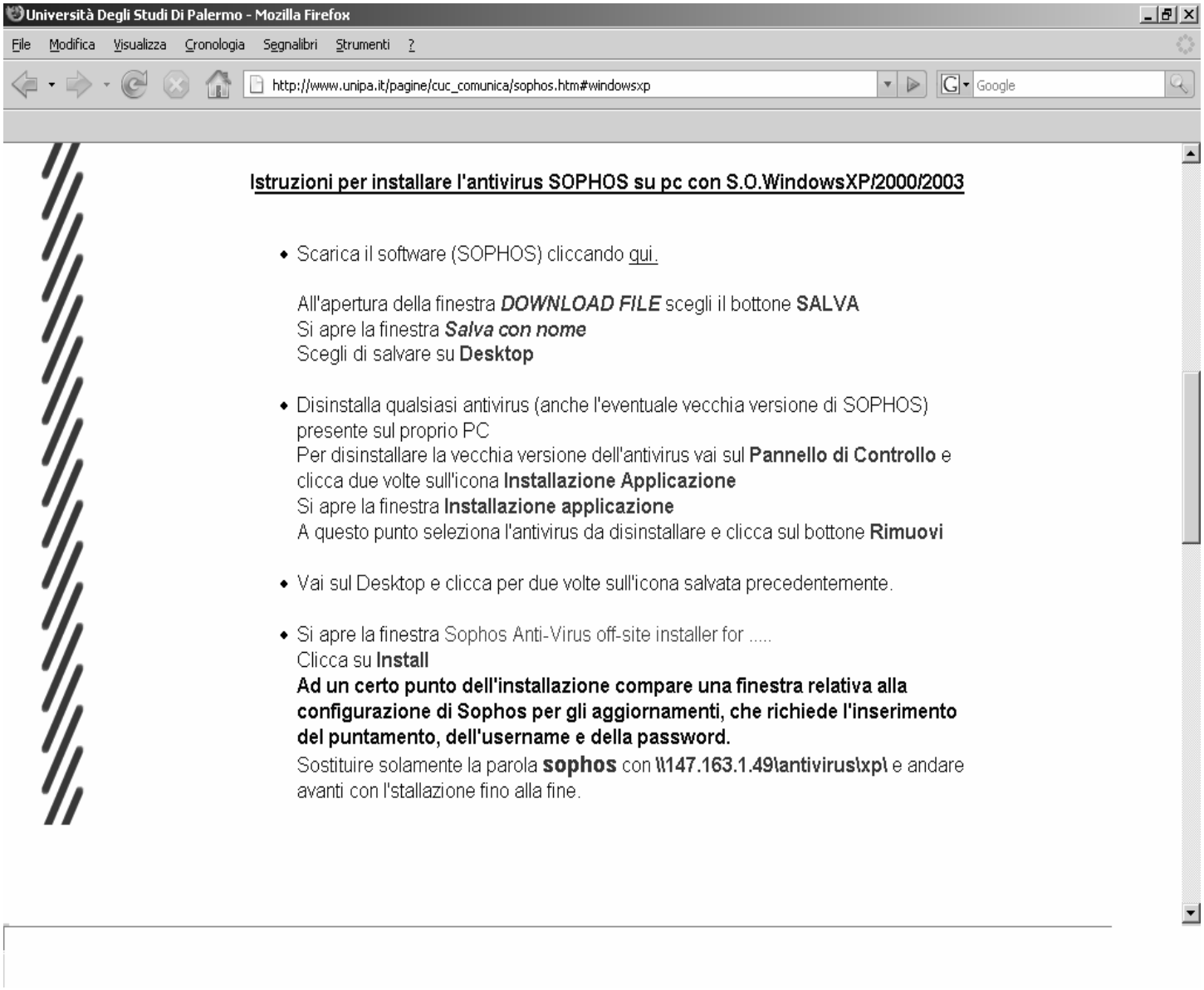
%

Il Phishing è una attività illegale, che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.

Antivirus
e tools rimozione malware

- Sophos
- Spybot Search and Destroy

%


Università Degli Studi Di Palermo - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
http://www.unipa.it/pagine/cuc_comunica/sophos.htm#windowsxp
Google
Istruzioni per installare l'antivirus SOPHOS su pc con S.O.WindowsXP/2000/2003
Scarica il software (SOPHOS) cliccando qui.
All'apertura della finestra DOWNLOAD FILE scegli il bottone SALVA
Si apre la finestra Salva con nome
Scegli di salvare su Desktop
Disinstalla qualsiasi antivirus (anche l'eventuale vecchia versione di SOPHOS) presente sul proprio PC
Per disinstallare la vecchia versione dell'antivirus vai sul Pannello di Controllo e clicca due volte sull'icona Installazione Applicazione
Si apre la finestra Installazione applicazione
A questo punto seleziona l'antivirus da disinstallare e clicca sul bottone Rimuovi
Vai sul Desktop e clicca per due volte sull'icona salvata precedentemente.
Si apre la finestra Sophos Anti-Virus off-site installer for .....
Clicca su Install
Ad un certo punto dell'installazione compare una finestra relativa alla configurazione di Sophos per gli aggiornamenti, che richiede l'inserimento del puntamento, dell'username e della password.
Sostituire solamente la parola sophos con \\147.163.1.49\antivirus\xp\ e andare avanti con l'stallazione fino alla fine.

%

Sophos


Updating Sophos Anti-Virus for Windows 2000/XP/2...
Downloading package 2 of 3...
Cancel
No files needed updating
15:10

Spybot

Spybot è un software che trova e rimuovere Spyware, Dialers, Malware e Hijackers eventualmente presenti sul vostro computer.

Cosa è lo spyware ?

La fonte dello spyware in origine era rappresentata esclusivamente da alcuni files che venivano inseriti sul nostro computer al momento di installare alcuni programmi (in genere programmi gratuiti). Il compito di tali spy, consiste nel raccogliere informazioni sull'utente, sull'Hardware e il Software presente sul PC, sulle abitudini di navigazione, sui siti visitati, sulla frequenza con il quale essi vengono visitati, sui Banner cliccati, sui tipi di acquisti effetuati online.

Gli Spyware tra possono spedire mail (SPAM) con il Vs. Account, prelevato dalle configurazioni di outlook o altri mail reader.

Gli Spyware (Malware-Hijacker). si installano, semplicemente navigando su siti a rischio (o anche in apparenza tranquilli) installando P2P.

Alcuni sono più invadenti di altri e possono arrivare a modificare permanentemente la vostra pagina iniziale del Browser (Hijacker) per proporne un altra (il cosidetto dirottamento) sostituire il motore di ricerca predefinito con un altro, potete ritrovarvi inserite nel Browser delle (Toolbar barre degli strumenti) che non avete chiesto di installare, ritrovarvi su siti pornografici o riguardanti casinò online. Molte di queste minacce sono spesso installate sul vostro PC tramite un controllo ActiveX. Oltre a ledere la vostra privacy, effetti collaterali dei programmi spyware sono il rallentamento anche notevole della vostra navigazione e possono anche creare conflitti e/omalfunzionamenti con altro software presente sul vostro computer.

%

Per quel che riguarda lo spyware, nulla a che vedere con virus, trojan o pirati informatici ma solo una raccolta di dati (Marketing) che poi viene rivenduta ad aziende specializzate. Un tempo questi file spyware, venivano sempre installati all'insaputa dell'utente ma oggi in molti casi c'è più trasparenza e ne viene fatta menzione nella licenza d'uso da accettare prima dell'installazione di alcuni software. Ma quanti di voi leggono per intero tale licenza al momento di installare un software?.

Visto che lo spyware con il tempo ha assunto una pseudo-legalità ecco comparire con il termine malware che va a identificare (a differenza dello spyware) tutto quello che si installa all'insaputa dell'utente e senza la sua autorizzazione.

%

Consigli per la protezione della postazione di lavoro

Effettuare gli aggiornamenti del sistema operativo;

- installare Sophos antivirus;
- installare SpyBot Search and Destroy;
- non aprire mail di dubbia provenienza;
- installare la password di BIOS del pc;
- installare un account utente limitato, in modo da limitare gli accessi come amministratore del computer;
- configurare lo screen saver, per bloccare automaticamente il pc in caso di assenza dalla propria postazione;
- non condividere mai le password personali (mail, password di accensione del pc, applicazione amministrativa, etc…);

%

- utilizzare password di almeno 8 caratteri NON riconducibili alla propria persona o a un familiare;
- utilizzare il proxy indicato dal proprio amministratore di sistema;
- effettuare la scansione dei supporti-dati con Sophos e Spybot;
- non effettuare l'installazione di software P2P se non strettamente necessario per fini didattici e/o ricerca;
- per qualsiasi dubbio rivolgersi all’amministratore di sistema della propria struttura.