

SOPHOS

Sophos Client Firewall, versione 1.5 manuale utente

Per Windows

Data documento: giugno 2007



Sommario

1	Per iniziare.....	4
2	Configurazione del firewall.....	12
3	Configurazione di reportistica e log.....	26
4	Modalità interattiva.....	28
5	Utilizzo del visualizzatore del log.....	34
6	Glossario.....	39
	Index	40

1 Per iniziare

Per iniziare

Questa sezione spiega come impostare e modificare le impostazioni della chiave per Sophos Client Firewall.

- [Per iniziare](#)
- [Interfaccia del firewall](#)
- [Icona nell'area di notifica](#)
- [Consenso all'utilizzo di un browser web](#)
- [Consenso all'utilizzo della posta elettronica](#)
- [Consenso alla condivisione file e stampanti](#)
- [Utilizzo interattivo del firewall](#)
- [Attivazione e disattivazione del firewall](#)

Per iniziare

Dopo la prima installazione del firewall può essere necessario configurarlo per consentire l'accesso alla rete alle applicazioni più comuni. Ciò dipende dal modo in cui il firewall è stato installato. Le installazioni possibili sono due:

- installazione e gestione dalla console di gestione centralizzata
- installazione autonoma.

Di seguito vengono forniti i relativi consigli per iniziare.

Installazione e gestione del firewall dalla console di gestione centralizzata.

Se il firewall viene installato e gestito dalla console di gestione centralizzata, blocca o consente il traffico secondo le regole stabilite dall'amministratore.

A meno che l'amministratore non abbia posto il firewall in modalità interattiva, l'utente non dovrebbe ricevere alcuna richiesta su come procedere.

Installazione autonoma del firewall

Se il firewall non è gestito dalla console centralizzata, chiede all'utente se bloccare o consentire il traffico per il quale non esistono delle regole. Questa è la "modalità interattiva".

Vedere [Modalità interattiva](#) per ulteriori informazioni su come gestire i

messaggi provenienti dal firewall.

In qualsiasi momento è possibile anche creare regole per permettere alle applicazioni più comuni di:

- consentire l'utilizzo di un browser web
- consentire la posta elettronica
- consentire la condivisione file e stampanti

Quando il firewall è stato configurato per riconoscere le applicazioni utilizzate dall'utente, è consigliabile porlo in modalità non interattiva. Vedere Selezione della modalità interattiva o non interattiva.

Interfaccia del firewall

Le aree principali dell'interfaccia del firewall sono le seguenti.

- **Editor configurazione di Sophos Client Firewall:** vedere Configurazione del firewall per ulteriori informazioni.
- **Visualizzatore del log:** vedere Introduzione al visualizzatore del log per ulteriori informazioni.
- Icona nell'area di notifica

Icona nell'area di notifica

Ciò che vede l'utente dipende dal gruppo di utenti in cui è stato inserito dall'amministratore di sistema.

- I membri dei gruppi **Sophos Administrator** e **SophosPowerUser** vedono l'icona, tutte le opzioni di menu e tutte le pagine dell'editor di configurazione.
- I membri dei gruppi **SophosUser** vedono l'icona, tutte le opzioni di menu e le quattro schede dell'editor di configurazione relative alle regole (Regole globali, Applicazioni, Processi e Checksum).
- Gli **utenti protetti** (che non siano membri di alcun gruppo Sophos) vedono l'icona e tre opzioni di menu (?, Informazioni su e Cancella allarme) e non hanno accesso all'editor di configurazione.

Quando il firewall è disattivato, nell'area di notifica l'icona del firewall è di colore grigio.



Quando il firewall è attivato, nell'area di notifica l'icona del firewall è di colore blu.

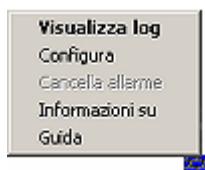


Quando il firewall è abilitato e un'applicazione non autorizzata tenta di accedere alla rete, l'icona del firewall nell'area di notifica diventa rossa. Il nome dell'applicazione bloccata appare nella descrizione dell'icona. Una volta selezionato dal menu Cancella allarme, l'icona diventa blu.



Se si clicca con il tasto destro del mouse sull'icona del firewall, è possibile selezionare le seguenti opzioni.

- **Visualizza log** per visualizzare il **Log di sistema**. Vedere [Introduzione al visualizzatore del log](#) per ulteriori informazioni.
- **Configura** per configurare l'**Editor configurazione di Sophos Client Firewall**. Vedere [Configurazione del firewall](#) per ulteriori informazioni.
- **Cancella allarme** per cancellare un allarme.
- **Informazioni su** per visualizzare informazioni sul prodotto.
- **?** per visualizzare il file della guida.



Consenso all'utilizzo di un browser web

Per consentire l'utilizzo di un browser web, procedere come segue.

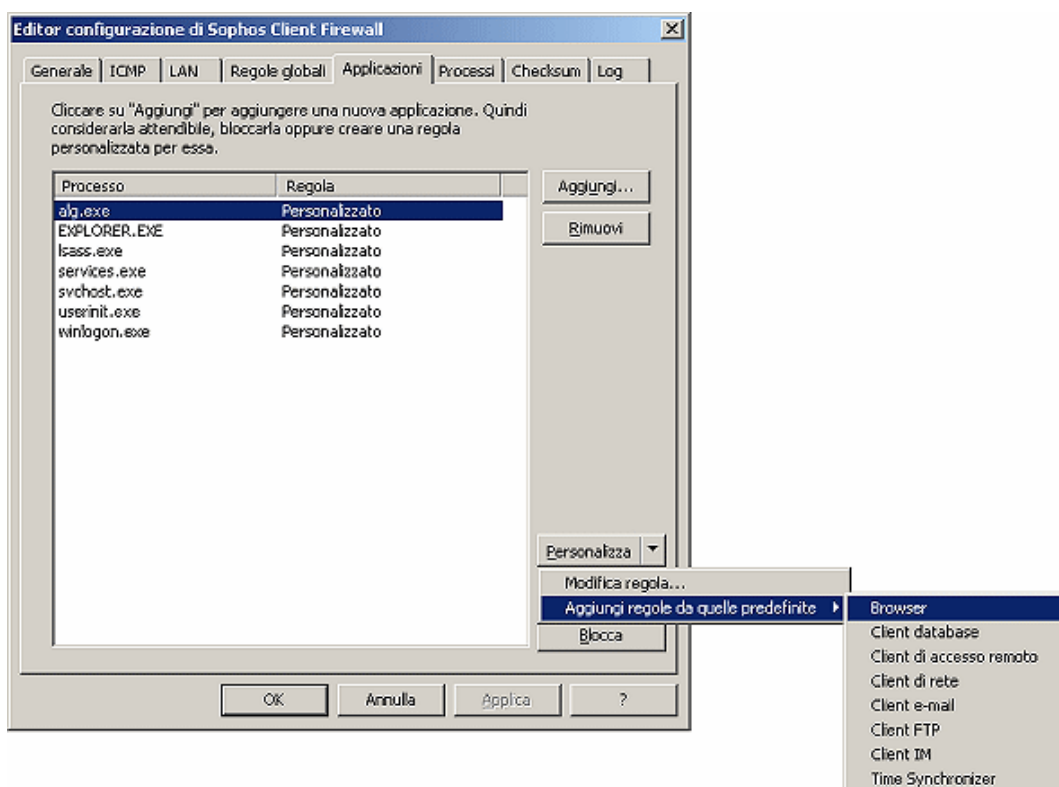
1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Applicazioni**. Cliccare su **Aggiungi** per cercare il browser sul computer, per esempio iexplore.exe per Internet Explorer. Il programma viene aggiunto alla lista ed è ora "Attendibile".

Per maggior sicurezza è consigliabile applicare una regola predefinita da Sophos. Evidenziare il programma, cliccare sulla freccia del menu a discesa posta sul pulsante **Personalizza**, selezionare **Aggiungi regole da quelle predefinite**, quindi selezionare **Browser**.

Cliccare su **OK**.

💡 Se si desidera impostare una regola personalizzata per il programma browser, consultare la pagina della guida [Impostazione delle regole per le applicazioni](#).

💡 Quando si consente l'utilizzo di un browser web, si consente anche l'accesso FTP.



Consenso all'utilizzo della posta elettronica

Per consentire la posta elettronica, procedere come segue.

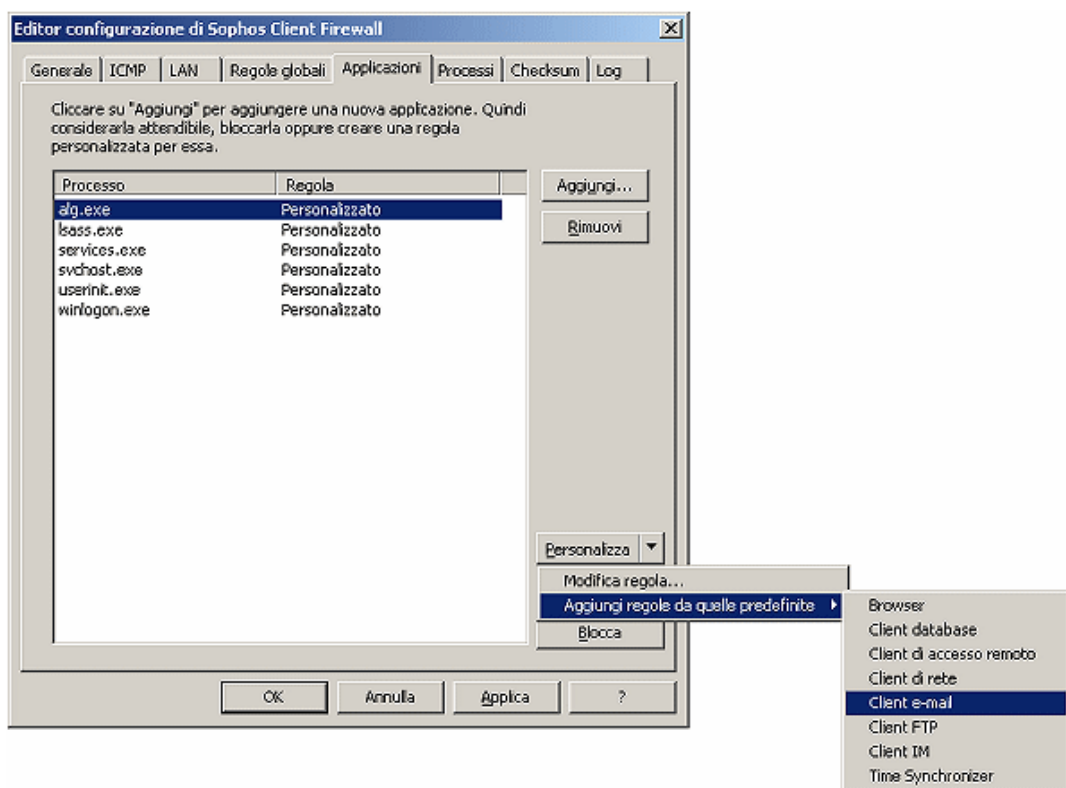
1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare Configura.
2. Nella finestra di dialogo Editor configurazione di Sophos Client Firewall, cliccare sulla scheda Applicazioni.
3. Cliccare su Aggiungi per cercare il programma di posta elettronica utilizzato dal computer. Il programma viene aggiunto alla lista ed è ora "Attendibile".

Per maggior sicurezza è consigliabile applicare una regola predefinita da Sophos. Evidenziare il programma, cliccare sulla freccia del menu a discesa posta sul pulsante **Personalizza**, selezionare **Aggiungi regole da quelle predefinite**, quindi selezionare **Client e-mail**.

Cliccare su **OK**.



Se si desidera impostare una regola personalizzata per il programma di posta elettronica, consultare la pagina della guida [Impostazione delle regole per le applicazioni](#).



Consenso alla condivisione file e stampanti

Per consentire la condivisione file e stampanti su una LAN (Rete di area locale), procedere come segue.

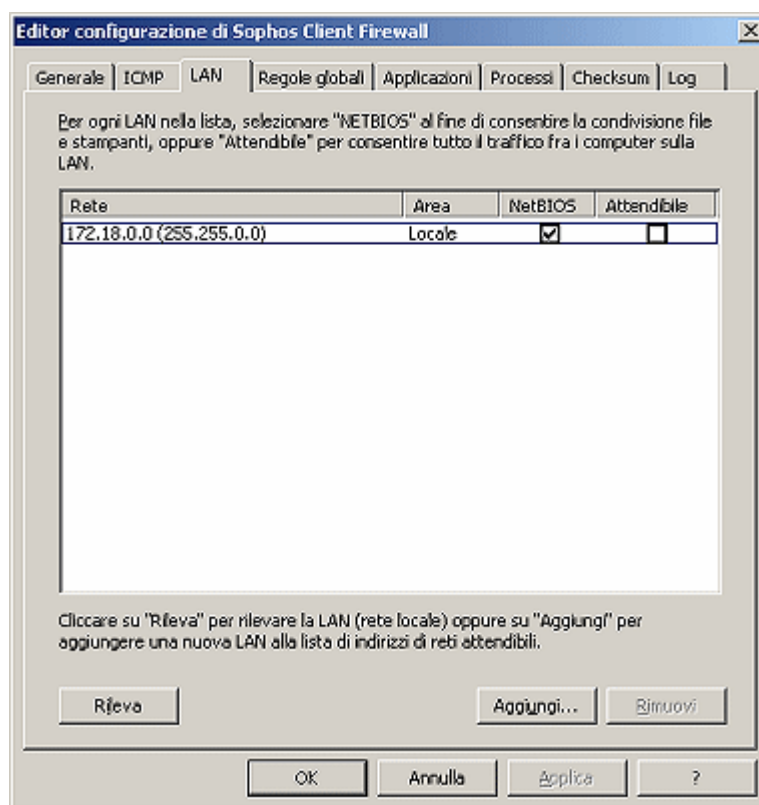
1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **LAN**.

3. Cliccare su **Rileva** per rilevare le LAN sulle quali si trova il computer e per aggiungerle automaticamente alla lista.

In alternativa, cliccare su **Aggiungi** per aggiungere una LAN alla lista. Viene visualizzata la finestra di dialogo Seleziona indirizzo. Utilizzarla per aggiungere nomi di dominio, numeri IP e indirizzi IP con maschera di sottorete. L'indirizzo di rete e la maschera di sottorete sono visualizzati nella colonna **Rete**, e il tipo di indirizzo di rete è visualizzato nella colonna **Area**.

Cliccare su **NetBIOS** per consentire la condivisione file e stampanti.

Cliccare su **OK**.



Utilizzo interattivo del firewall


Sophos Client Firewall può funzionare in due modalità diverse.


- **Interattiva.** Il firewall chiede all'utente come gestire il traffico.
- **Non interattiva.** Il firewall gestisce il traffico in modo automatico utilizzando le regole impostate.

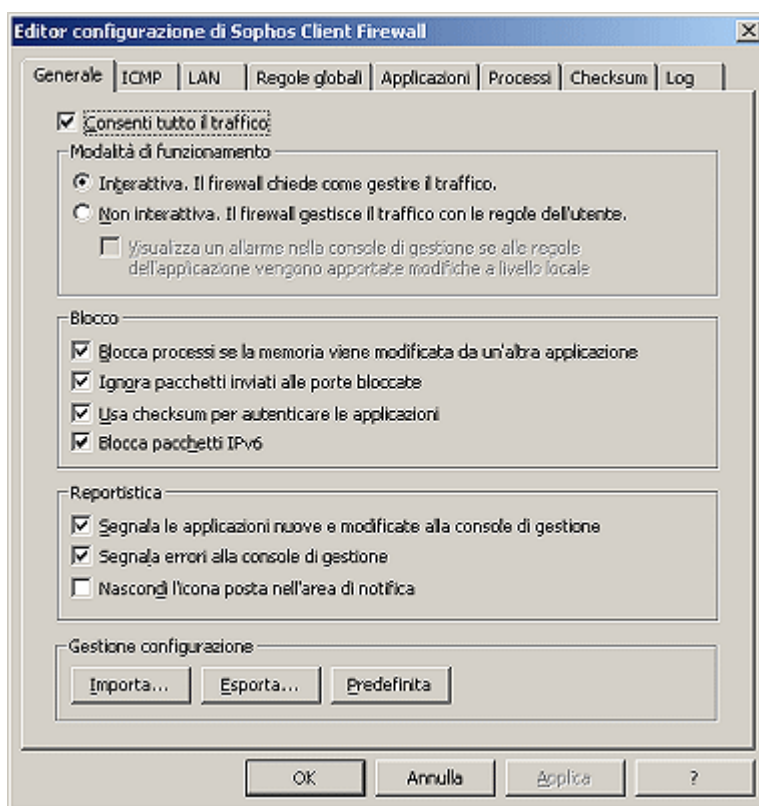
Per cambiare modalità di funzionamento, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Generale**.
3. Selezionare **Interattiva** o **Non interattiva**.

Cliccare su **OK**.

 Se si seleziona **Non interattiva**, è possibile anche selezionare l'opzione **Visualizza un allarme nella console di gestione se alle regole dell'applicazione vengono apportate modifiche a livello locale**. In questo modo, viene visualizzato un allarme nella console di gestione centralizzata (se utilizzata), nel caso in cui vengono apportate modifiche a una regola (ovvero regole delle applicazioni o regole globali, processi o checksum).

 Per ulteriori informazioni, vedere [Modalità interattiva](#).



Attivazione e disattivazione del firewall

Per impostazione predefinita il firewall è attivato, tuttavia è possibile consentire tutto il traffico.

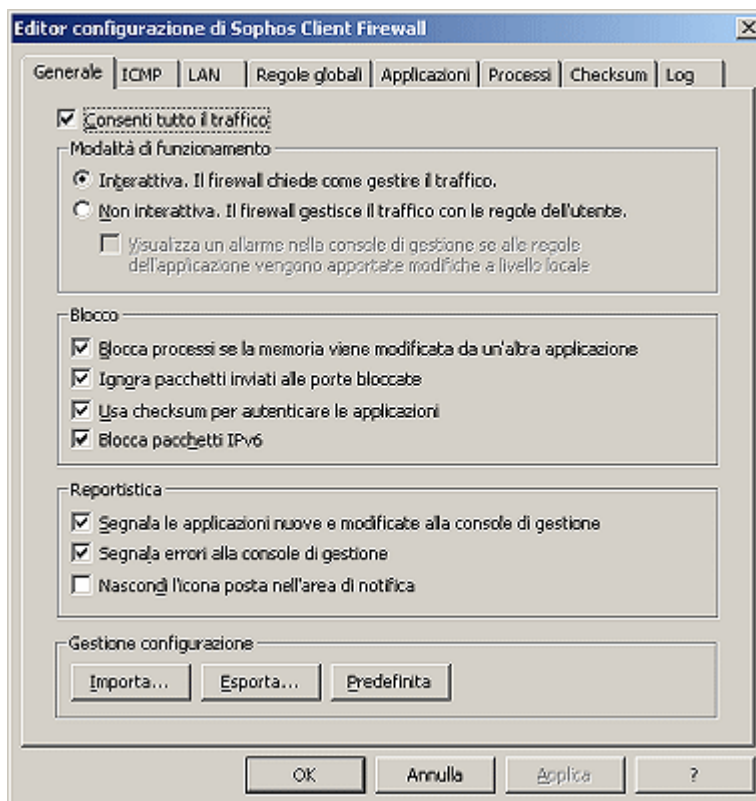
Per disattivare il firewall, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Generale**.
3. Selezionare **Consenti tutto il traffico**.

Cliccare su **OK**.



Per l'utilizzo quotidiano, si consiglia di tenere il firewall **attivato**.



2 Configurazione del firewall

Configurazione del firewall

È possibile configurare il firewall e poi attivarlo. Lo si può configurare in molti modi diversi utilizzando l'Editor configurazione di Sophos Client Firewall. Alcune funzioni comuni sono comunque elencate qui sotto.

- Selezione della modalità interattiva o non interattiva
- Consenso al traffico ICMP in ingresso e in uscita
- Consenso al traffico tra computer in una rete LAN
- Consenso al download FTP
- Impostazione delle regole globali
- Impostazione delle regole per le applicazioni
- Consenso all'avvio di processi nascosti da parte delle applicazioni
- Consenso all'utilizzo dei raw socket da parte delle applicazioni
- Utilizzo dei checksum per autenticare le applicazioni
- Importazione ed esportazione delle configurazioni esistenti
- Priorità delle regole

Selezione della modalità interattiva o non interattiva

Sophos Client Firewall può funzionare in due modalità diverse.

- **Interattiva.** Il firewall chiede all'utente come gestire il traffico.
- **Non interattiva.** Il firewall gestisce il traffico in modo automatico utilizzando le regole impostate.

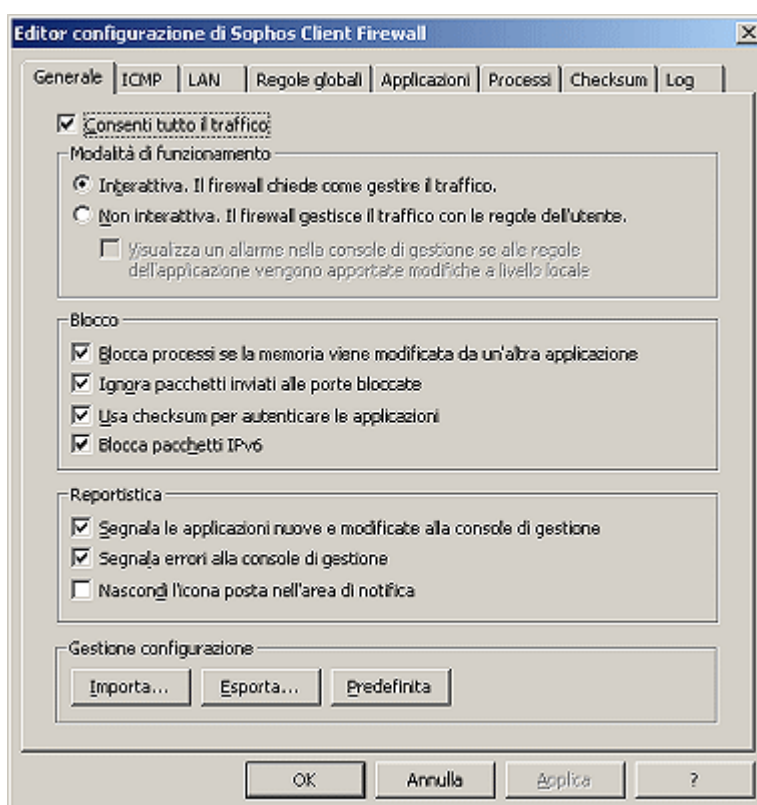
Per cambiare modalità di funzionamento, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Generale**.
3. Selezionare la modalità **Interattiva** o **Non interattiva**.

Cliccare su **OK**.



Se si seleziona **Non interattiva**, è possibile anche selezionare l'opzione **Visualizza un allarme nella console di gestione se alle regole dell'applicazione vengono apportate modifiche a livello locale**. In questo modo, viene visualizzato un allarme nella console di gestione centralizzata (se utilizzata), nel caso in cui vengono apportate modifiche a una regola (ovvero regole delle applicazioni o regole globali, processi o checksum).



Consenso al traffico ICMP in ingresso e in uscita



Si consiglia di specificare il tipo e la direzione dei messaggi ICMP solo se si è a conoscenza dei protocolli di rete.

Per specificare il tipo e la direzione dei messaggi ICMP, procedere come segue.

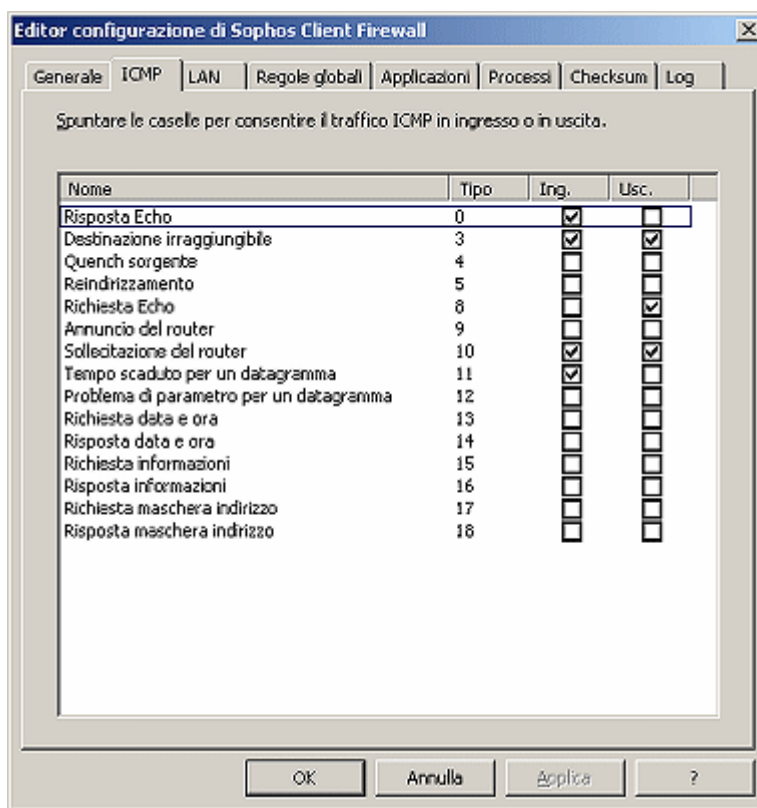
1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.

2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **ICMP**.
3. Cliccare su **Ing.** per autorizzare i messaggi in ingresso del tipo specificato.

Cliccare su **Usc.** per autorizzare i messaggi in uscita del tipo specificato.

Cliccare su **OK**.

Per ulteriori informazioni sul traffico ICMP cliccare qui. Per la definizione di traffico ICMP cliccare qui.



Consenso al traffico tra computer in una rete LAN

Per consentire tutto il traffico tra computer in una rete LAN, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **LAN**.

3. Cliccare su **Rileva** per rilevare le LAN sulle quali si trova il computer e per aggiungerle automaticamente alla lista.

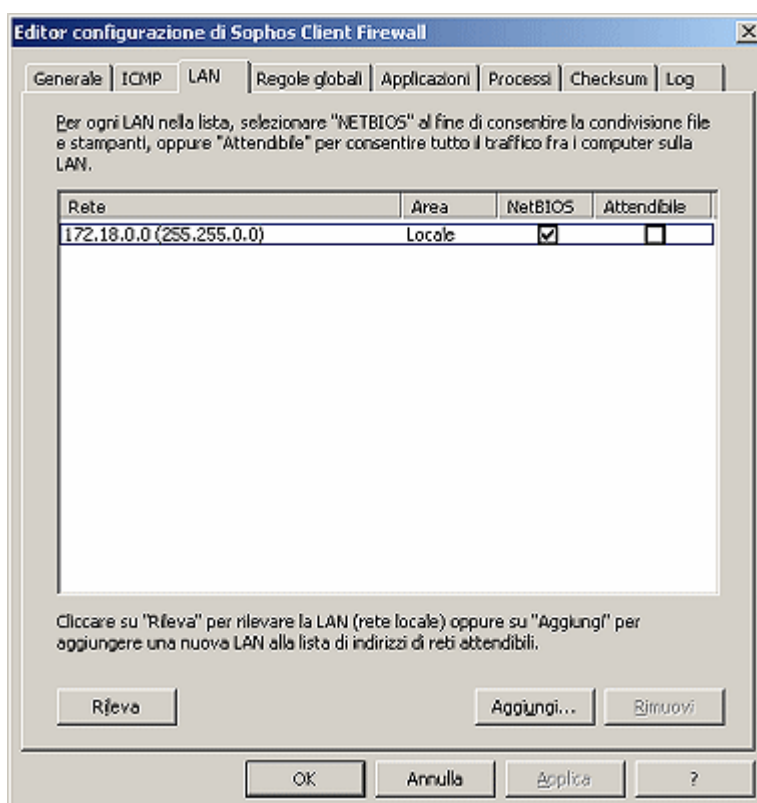
In alternativa, cliccare su **Aggiungi** per aggiungere una LAN alla lista. Viene visualizzata la finestra di dialogo Seleziona indirizzo. Utilizzarla per inserire l'indirizzo della LAN.

Cliccare su **Attendibile** per consentire il traffico tra computer su una LAN.


Cliccare su **OK**.



Se si clicca su **Attendibile**, ciò permette anche di selezionare l'opzione NetBIOS che abilita la condivisione file e stampanti.



Consenso al download FTP


 Se è stato consentito l'utilizzo di un browser web che può accedere ai server FTP, non è necessario consentire anche i download FTP.

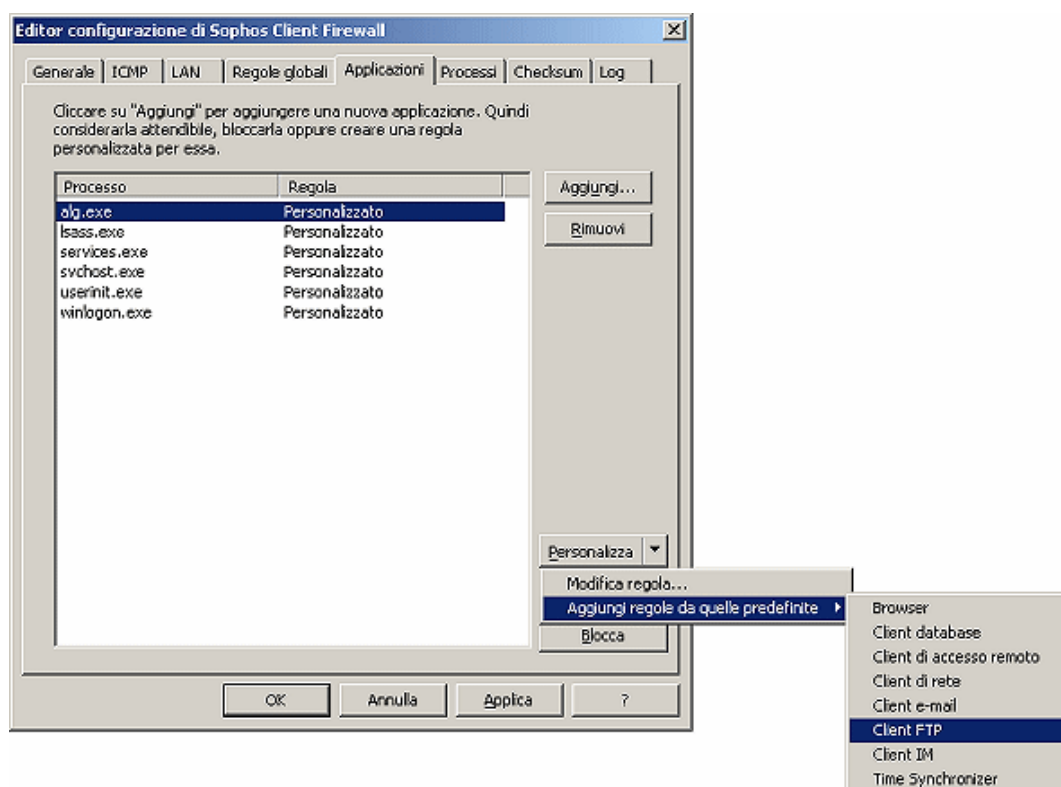
Per consentire i download FTP, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Applicazioni**. Cliccare su **Aggiungi** per cercare il programma utilizzato per i download FTP. Il programma viene aggiunto alla lista ed è ora "Attendibile".


Per maggior sicurezza è consigliabile applicare una regola predefinita da Sophos. Evidenziare il programma, cliccare sulla freccia del menu a discesa posta sul pulsante **Personalizza**, selezionare **Aggiungi regole da quelle predefinite**, quindi selezionare **Client FTP**.

Cliccare su **OK**.

 Se si desidera impostare una regola personalizzata per il programma FTP, consultare la pagina della guida [Impostazione delle regole per le applicazioni](#).



Impostazione delle regole globali

 Si consiglia di impostare una regola solo se si è a conoscenza dei protocolli di rete.



È possibile specificare **regole globali** che vengono applicate a tutte le comunicazioni di rete o alle applicazioni che non possiedono ancora una regola.

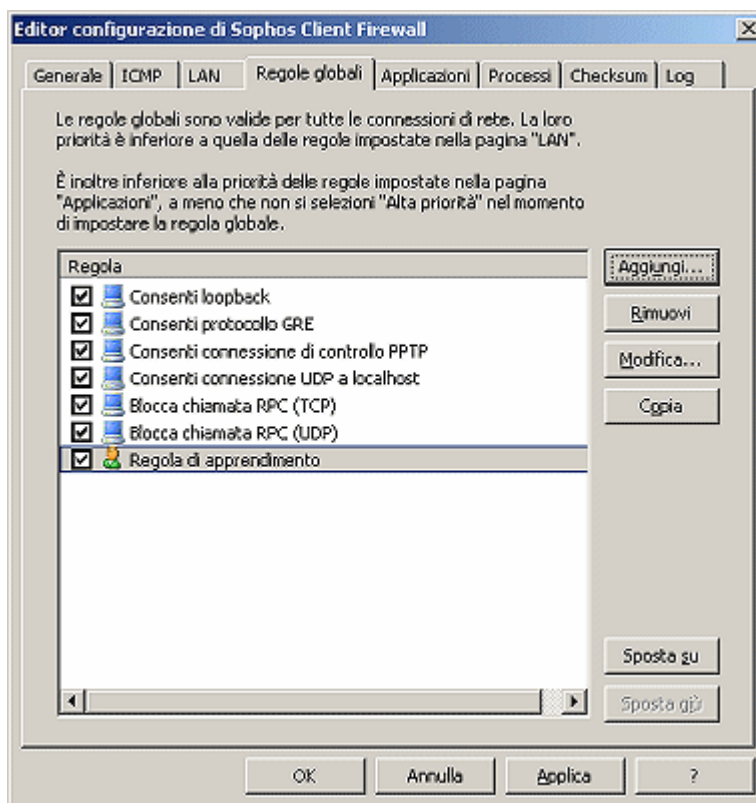
Per specificare e dare priorità alle regole globali, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Regole globali**.
3. Cliccare su **Aggiungi** per aggiungere una nuova regola alla lista. Vedere [Impostazione di una regola](#) per ulteriori informazioni.


Cliccare su **Sposta su** o **Sposta giù** per modificare la priorità della regola selezionata all'interno della lista.

Cliccare su **OK**.

-  Le regole globali hanno una priorità inferiore a quella delle regole impostate nelle schede LAN e Applicazioni, a meno che non si selezioni **Regola con elevata priorità**. Le regole a elevata priorità vengono applicate prima delle regole delle applicazioni.
-  Le regole predefinite e personalizzate vengono distinte con icone differenti. Se si tenta di modificare o cancellare una regola predefinita, compare un avviso.



Impostazione delle regole per le applicazioni

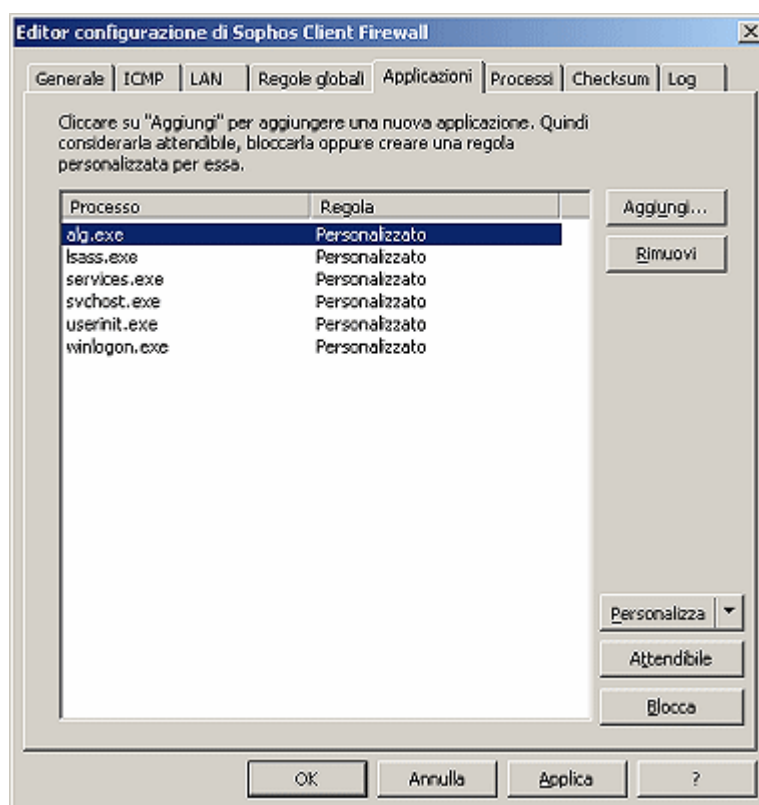
-  Si consiglia di impostare una regola solo se si è a conoscenza dei protocolli di rete.

È possibile impostare le regole riguardanti il modo in cui il firewall gestirà le applicazioni, nel modo seguente.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Applicazioni**. Cliccare su **Aggiungi** per cercare un'applicazione da aggiungere alla lista. L'applicazione è ora attendibile, vale a dire che ad essa è consentita tutta l'attività in rete.

Selezionare l'applicazione e cliccare su **Blocca** se si desidera bloccarla oppure su **Personalizza** se si desidera creare una regola che specifica quando l'applicazione può essere eseguita. Se si clicca su **Personalizza**, è possibile applicare una regola predefinita creata da Sophos oppure utilizzare **Modifica regola** per crearne una propria.

Cliccare su **OK**.



Consenso all'avvio di processi nascosti da parte delle applicazioni

A volte, un'applicazione avvia un processo nascosto che acceda alla rete per suo conto. Le applicazioni malevole possono utilizzare tale tecnica

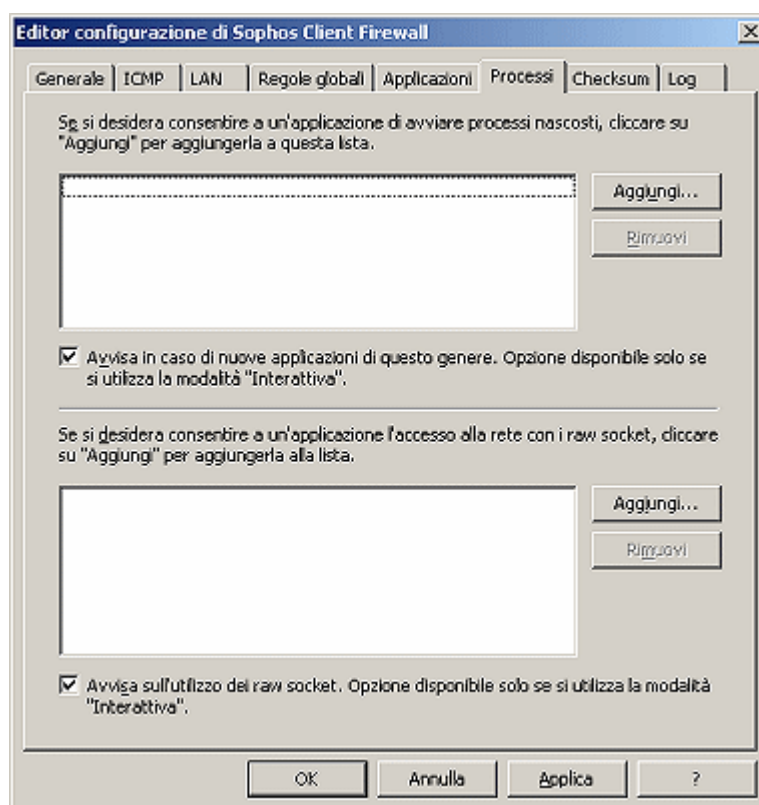
per eludere i firewall; anziché tentare l'accesso alla rete esse stesse avviano a questo scopo un'altra applicazione.

Per specificare e gestire applicazioni cui è consentito l'avvio di processi nascosti, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Processi**.
3. Cliccare sul pulsante **Aggiungi** situato accanto al campo elenco in alto per cercare un'applicazione, e aggiungerla quindi alla lista di applicazioni cui è consentito avviare processi nascosti.

Il firewall può informare l'utente in caso di rilevamento di una nuova applicazione che avvia processi nascosti. Selezionare **Avvisa in caso di nuove applicazioni di questo genere**. Quest'opzione è disponibile solo se si utilizza la modalità **Interattiva**. Se l'opzione non viene selezionata, alle nuove applicazioni in grado di avviare processi nascosti tale operazione non viene consentita.

Cliccare su **OK**.



Consenso all'utilizzo dei raw socket da parte delle applicazioni

Alcune applicazioni possono accedere a una rete tramite i raw socket, che permettono loro di controllare tutti gli aspetti relativi ai dati inviati dalle stesse applicazioni sulla rete. Le applicazioni malevole possono sfruttare i raw socket, per esempio falsificando il proprio indirizzo IP o inviando deliberatamente messaggi danneggiati.

Per specificare e gestire le applicazioni che utilizzano i raw socket, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Processi**.
3. Cliccare sul pulsante **Aggiungi** situato accanto al campo elenco in basso per cercare un'applicazione, e aggiungerla alla lista di applicazioni cui è consentito utilizzare i raw socket.

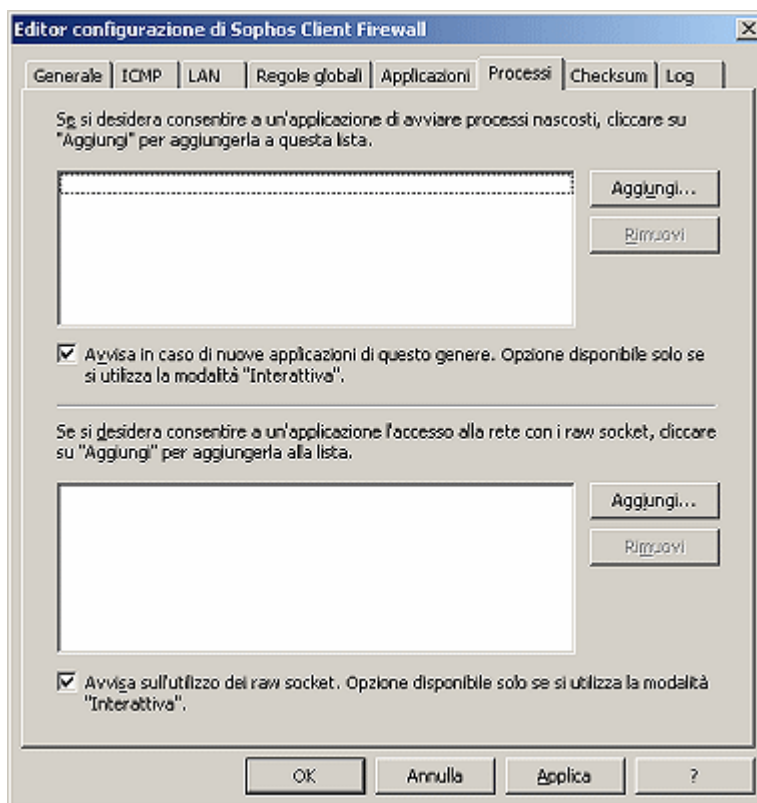
Se si utilizza la modalità interattiva, il firewall può informare l'utente del rilevamento di un raw socket, purché sia stata selezionata l'opzione

Avvisa sull'utilizzo dei raw socket. **Quest'opzione è disponibile solo se si utilizza la modalità "interattiva"**. Se l'opzione non è selezionata, tutte le applicazioni che utilizzano i raw socket vengono bloccate.

Cliccare su OK.



Per ricevere tali avvisi, è necessario selezionare la modalità **Interattiva** nella scheda **Generale**.



Utilizzo dei checksum per autenticare le applicazioni

Ogni versione di un'applicazione ha un checksum unico. Il firewall può utilizzare tale checksum per decidere se consentire o meno un'applicazione.

Per impostazione predefinita, il firewall controlla il checksum di ciascuna applicazione che viene eseguita. Se il checksum è sconosciuto o è cambiato, il firewall lo blocca oppure (nella modalità interattiva) chiede all'utente cosa fare e cambia il colore dell'icona posta nell'area di

notifica in rosso. Inoltre, al primo rilevamento di un'applicazione nuova o modificata, il firewall invia un allarme alla console di gestione, se utilizzata.

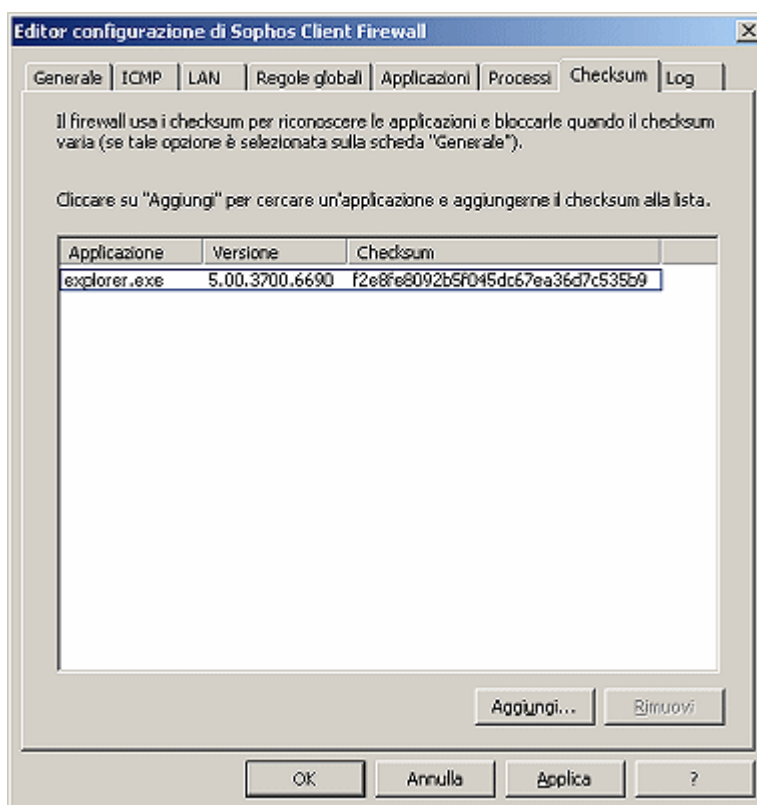
È possibile aggiungere un checksum alla lista di quelli consentiti, nel modo seguente.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare su **Checksum**.
3. Per aggiungere un checksum cliccare su **Aggiungi** e selezionare un'applicazione.

Cliccare su **OK**.



Verificare che l'opzione **Utilizza checksum per autenticare le applicazioni** sia selezionata nella scheda **Generale**.



Importazione ed esportazione delle configurazioni esistenti

È possibile importare o esportare delle configurazioni che sono già state create.

Per esempio, si possono creare delle regole per le applicazioni su un computer e poi esportare tale configurazione per utilizzarla in un altro computer che esegue lo stesso gruppo di applicazioni.

È possibile anche prelevare configurazioni create su diversi computer, importarle nella console di amministrazione centrale e unirle per creare un criterio valido per tutti i computer sulla rete.

Per gestire i file di configurazione, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica, e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Generale**.
3. Per importare un criterio cliccare su **Importa**. Nella finestra di dialogo **Importa configurazione** selezionare un file di configurazione e cliccare su **Apri**. Compare una finestra.

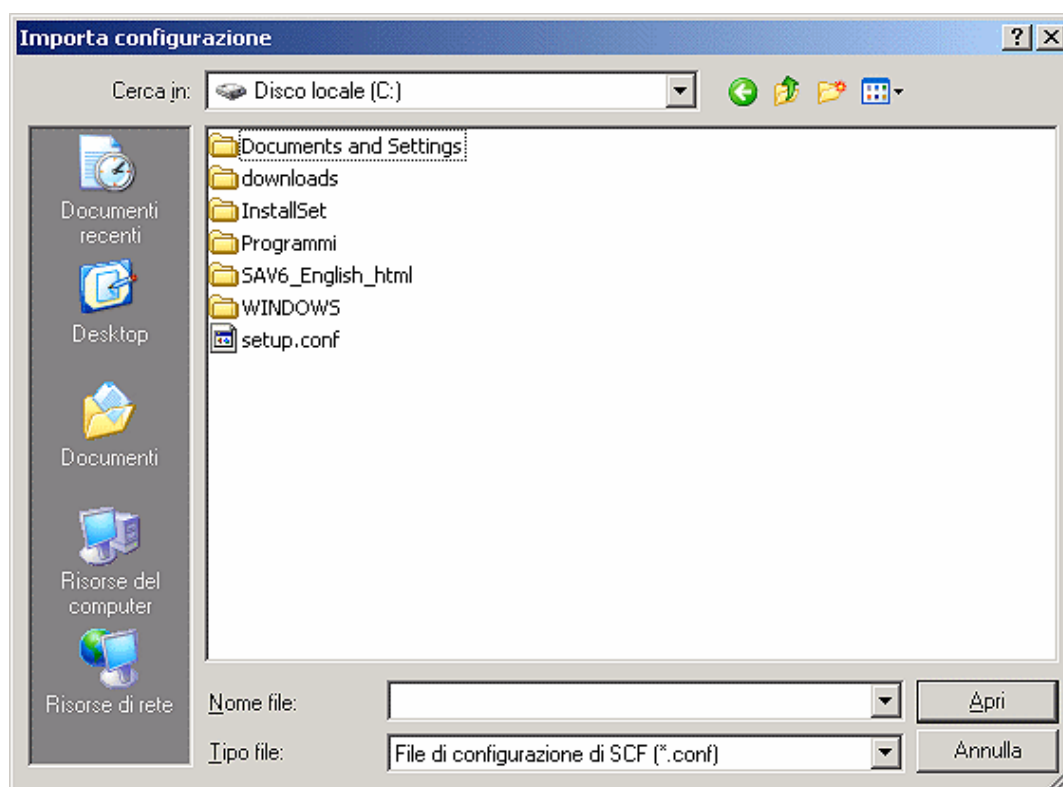
Spuntare la casella **Caricare configurazione generale e/o Caricare regole globali e regole applicazioni**.

Se si è spuntata la casella **Caricare regole globali e regole applicazioni**, selezionare il pulsante di opzione **Unire** o **Sovrascrivere**. Cliccare su **OK**.

Per esportare un criterio cliccare su **Esporta**. Nella finestra di dialogo **Esporta configurazione**, assegnare un nome e un percorso alla configurazione e cliccare su **Salva**.

Per ripristinare la configurazione predefinita cliccare su **Predefinita**. Compare una finestra con il messaggio **Ripristinare le impostazioni predefinite?** Cliccare su **Sì** per completare l'operazione.

Cliccare su **OK**.



Priorità delle regole

Per le connessioni che non utilizzano i raw socket (la maggior parte), le diverse regole vengono controllate nel seguente ordine.

1. Se la connessione è con un indirizzo contrassegnato come attendibile e contenuto in uno degli intervalli specificati nella scheda delle proprietà della LAN, la connessione viene consentita senza ulteriori controlli.
2. Se la rete ammette solo NetBIOS, viene consentita qualsiasi connessione che soddisfa i seguenti criteri.
 - ▶ Qualsiasi connessione TCP dove la porta remota è compresa nell'intervallo 137-139 o è 445.
 - ▶ Qualsiasi connessione TCP dove la porta locale è compresa nell'intervallo 137-139 o è 445.
 - ▶ Qualsiasi connessione UDP dove la porta remota è 137 o 138.
 - ▶ Qualsiasi connessione UDP dove la porta locale è 137 o 138.
3. Le regole globali a elevata priorità vengono controllate nell'ordine in cui sono elencate.

4. Se la connessione non è stata già gestita (vale a dire se non vi sono state applicate regole), il firewall controlla le regole dell'applicazione.
5. Se la connessione non è stata ancora gestita il firewall applica a essa le regole globali a priorità normale.
6. Se non viene trovata alcuna regola per gestire la connessione e il firewall si trova in modalità interattiva, all'utente verrà chiesto come procedere.

3 Configurazione di reportistica e log

Configurazione di reportistica e log

- [Configurazione della reportistica centrale](#)
- [Configurazione del log](#)

Configurazione della reportistica centrale

Per impostazione predefinita, il firewall riporta alla console di gestione centralizzata (se utilizzata per gestire il firewall) i seguenti eventi:

- applicazioni nuove e modificate
- errori

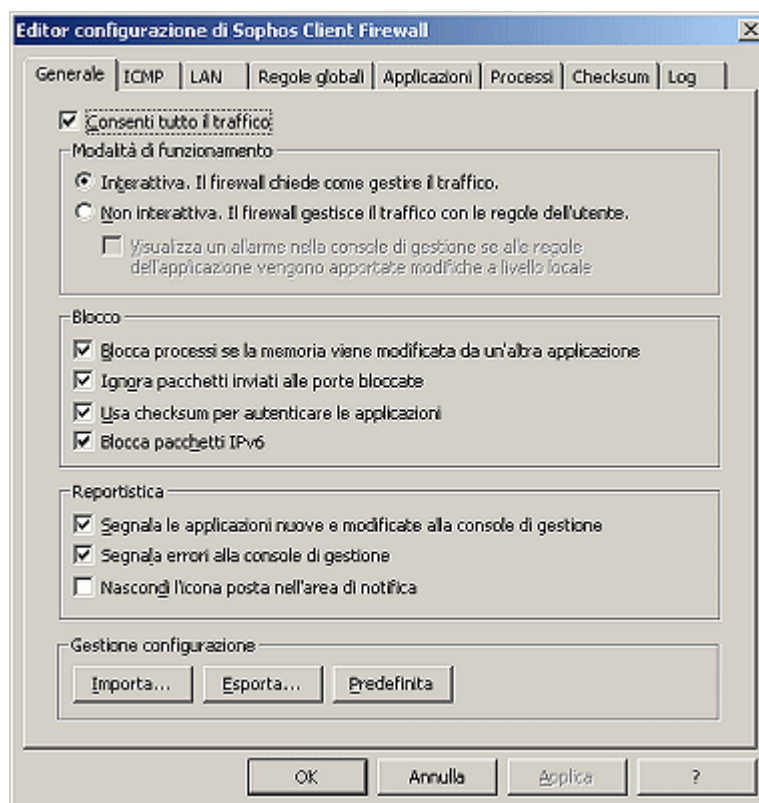
Per cambiare le impostazioni della reportistica, procedere come segue.

1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Generale**. Nel riquadro **Reportistica**, abilitare o disabilitare ciascun tipo di reportistica.

Cliccare su **OK**.



Sophos Client Firewall può segnalare le applicazioni nuove e modificate solo se, in questa scheda, è selezionata l'opzione **Utilizza checksum per autenticare le applicazioni**.



Configurazione del log

Per gestire dimensioni e contenuto del database del log degli eventi procedere come segue.

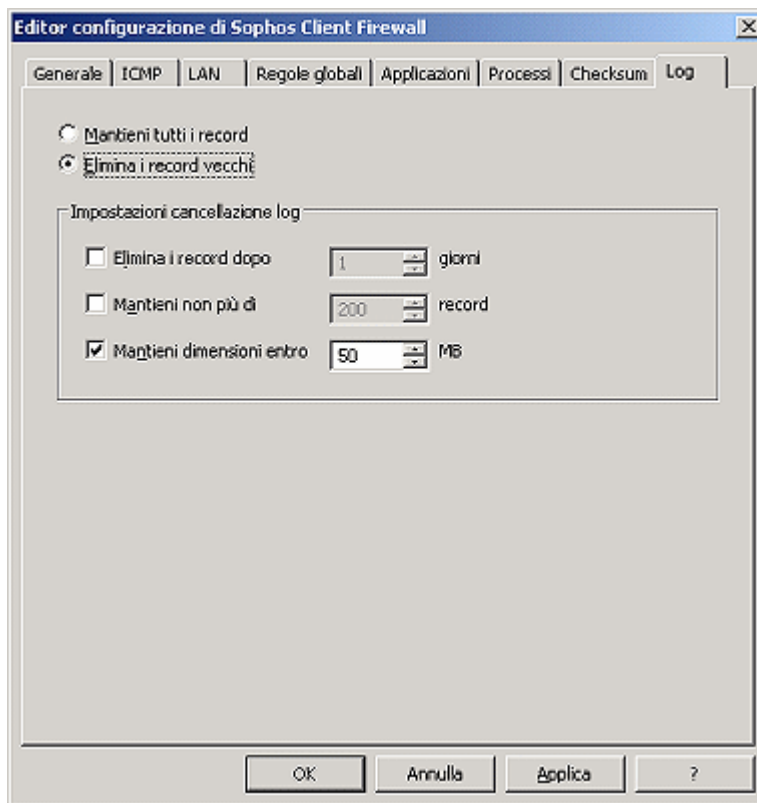
1. Cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica e selezionare **Configura**.
2. Nella finestra di dialogo **Editor configurazione di Sophos Client Firewall**, cliccare sulla scheda **Log**.
3. Per permettere al database di crescere in modo illimitato, cliccare su **Mantieni tutti i record**.

Per cancellare i record obsoleti, quando le dimensioni del log raggiungono i limiti specificati nel pannello di controllo **Impostazioni cancellazione log**, cliccare su **Elimina i record vecchi**. Questa è l'opzione predefinita.

Per stabilire le **Impostazioni cancellazione log** selezionare una o più delle seguenti opzioni.

- ▶ Spuntare la casella **Elimina i record dopo** e inserire o selezionare una cifra nel campo **giorni**. Quest'opzione è deselezionata per impostazione predefinita.
- ▶ Spuntare la casella **Mantieni non più di** e inserire o selezionare una cifra nel campo **record**. Quest'opzione è deselezionata per impostazione predefinita.
- ▶ Spuntare la casella **Mantieni dimensioni entro** e inserire o selezionare una cifra nel campo **MB**. Quest'opzione è selezionata per impostazione predefinita e le dimensioni sono impostate inizialmente su 50 MB.

Cliccare su **OK**.



4 Modalità interattiva

Modalità interattiva

Se si utilizza la **modalità interattiva** il firewall avvisa l'utente ogni volta che un'applicazione sconosciuta richiede l'accesso alla rete. Il firewall

quindi chiede all'utente se deve consentire il traffico una volta, bloccarlo una volta o se creare una regola per quel tipo di traffico.

Verranno visualizzati i seguenti tipi di messaggi.

- Messaggio di processo nascosto
- Messaggio sul protocollo
- Messaggio sull'applicazione
- Messaggio sui raw socket
- Messaggio sulle applicazioni nuove o modificate

Messaggio di processo nascosto

Un processo nascosto si verifica quando un'applicazione ne avvia un'altra che accede alla rete per conto della prima. Le applicazioni malevole utilizzano tale tecnica per eludere i firewall; anziché tentare l'accesso alla rete esse stesse avviano a questo scopo un'applicazione attendibile.

La finestra a comparsa indica il processo nascosto e l'applicazione che l'ha avviata.

Selezionare una delle seguenti opzioni:

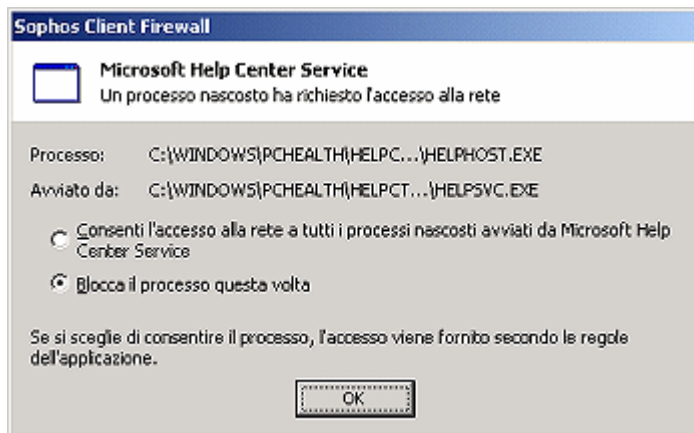
Consenti l'accesso alla rete a tutti i processi nascosti avviati da ...
aggiunge una nuova regola e consente a questa applicazione di avviare processi nascosti.

Blocca il processo questa volta nega l'accesso per questo specifico processo, solo una volta. Questa è l'opzione predefinita e sarà selezionata anche premendo il tasto Esc.

Cliccare su OK.



Questa finestra a comparsa viene visualizzata soltanto se è stata selezionata l'opzione **Avvisa in caso di nuove applicazioni di questo genere** nella scheda **Processi**.



Messaggio sul protocollo

Occasionalmente il firewall rileva un'attività in rete da parte del sistema, non connessa a una specifica applicazione. In questo caso chiede di creare una regola per il protocollo.

La finestra a comparsa mostra l'attività di rete non riconosciuta, vale a dire il protocollo e l'indirizzo remoto.

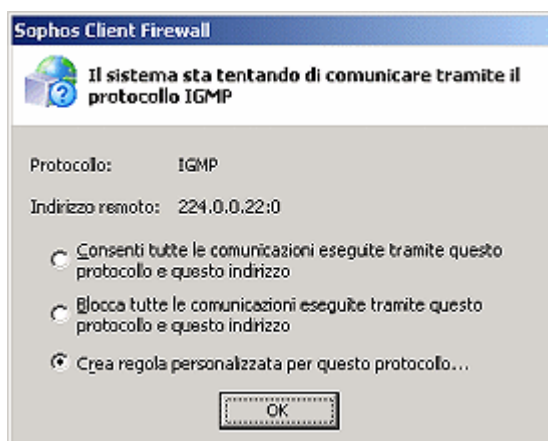
Selezionare una delle seguenti opzioni:

Consenti tutte le comunicazioni eseguite tramite questo protocollo e questo indirizzo aggiunge una regola per consentire la comunicazione con l'indirizzo specificato tramite il protocollo indicato.

Blocca tutte le comunicazioni eseguite tramite questo protocollo e questo indirizzo aggiunge una regola per bloccare le comunicazioni con l'indirizzo specificato tramite il protocollo indicato. Se si preme il tasto Esc, si blocca la comunicazione tramite il protocollo e l'indirizzo specificati soltanto in questa occasione.

Crea regola personalizzata per questo protocollo consente di creare una regola personalizzata (per consentire o bloccare le comunicazioni). Questa è l'opzione predefinita. Vedere [Impostazione di una regola](#) per ulteriori informazioni.

Cliccare su OK.



Messaggio sull'applicazione

Se il firewall rileva che un'applicazione sta tentando di accedere alla rete in modo non previsto da alcuna regola, chiede la creazione di una regola per l'applicazione stessa.

La finestra a comparsa mostra l'attività di rete non riconosciuta, vale a dire il servizio e l'indirizzo remoti.

Selezionare una delle seguenti opzioni:

Consenti tutte le attività per questa applicazione solo questa volta consente questa particolare connessione solo una volta. Dato che tale opzione non crea una regola, il messaggio verrà visualizzato di nuovo al prossimo tentativo di connessione.

Consenti tutte le attività per questa applicazione crea una semplice regola di applicazione che consente a quest'ultima l'accesso illimitato alla rete.

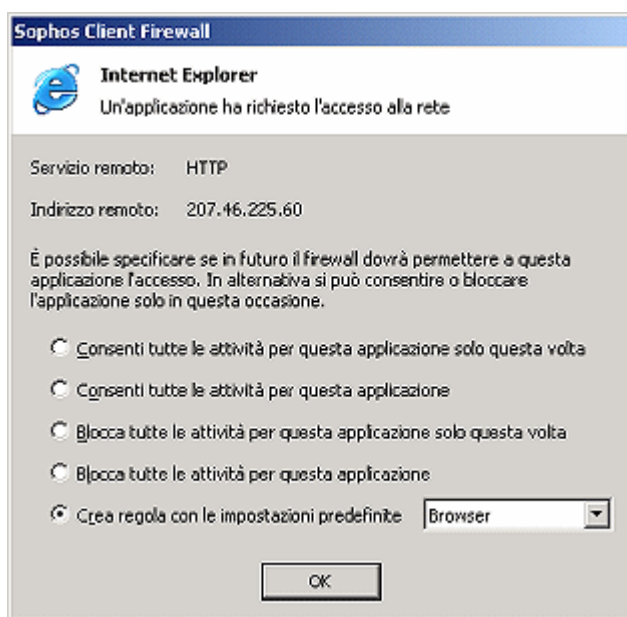
Blocca tutte le attività per questa applicazione solo questa volta blocca questa particolare connessione solo una volta. Dato che tale opzione non crea una regola, il messaggio verrà visualizzato di nuovo al prossimo tentativo di connessione. Questa opzione sarà selezionata anche premendo il tasto Esc.

Blocca tutte le attività per questa applicazione crea una semplice regola di applicazione che nega a quest'ultima qualsiasi accesso alla rete.

Crea regola con le impostazioni predefinite consente di selezionare una regola predefinita configurata da Sophos. In alternativa, cliccare su

Personalizza... per creare una propria regola. Vedere [Impostazione di una regola](#) per ulteriori informazioni.

Al termine dell'operazione, cliccare su **OK**.



Messaggio sui raw socket

I **raw socket** consentono ai processi di controllare tutti gli aspetti dei dati che inviano attraverso la rete e possono essere utilizzati per scopi malevoli. È possibile gestire i raw socket rispondendo alla finestra a comparsa visualizzata dal firewall quando non c'è alcuna regola per consentire l'accesso a un particolare raw socket.

La finestra a comparsa mostra i dati relativi al raw socket.


Selezionare una delle seguenti opzioni:

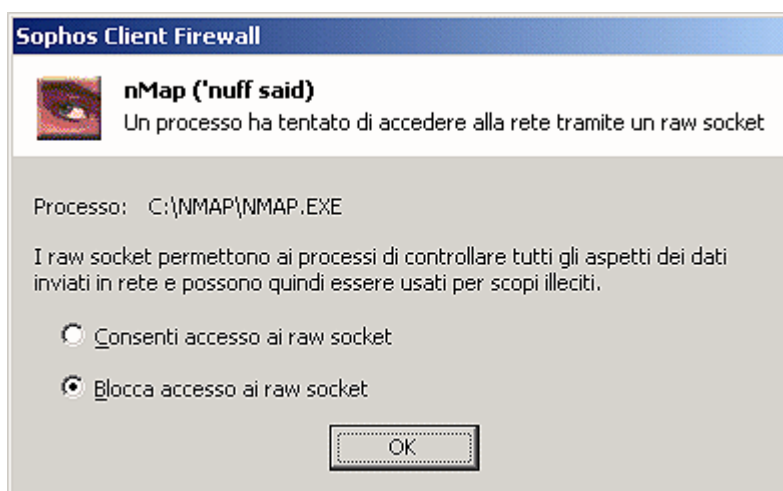
Consenti accesso ai raw socket aggiunge una regola per consentire a questa applicazione l'utilizzo dei raw socket (vale a dire l'accesso illimitato alla rete).

Blocca accesso ai raw socket blocca l'accesso alla rete da parte di questa istanza del processo. Dato che tale opzione non aggiunge una regola, il messaggio verrà visualizzato di nuovo la prossima volta che l'applicazione verrà eseguita. Questa è l'opzione predefinita e sarà

selezionata anche premendo il tasto Esc.

Cliccare su OK.

 Questa finestra a comparsa viene visualizzata solo se è stata spuntata la casella **Avvisa sull'utilizzo dei raw socket** nella pagina **Processi**.



Messaggio sulle applicazioni nuove o modificate

Se il firewall rileva un'applicazione nuova o modificata, visualizza un messaggio (purché sia stata selezionata l'opzione **Utilizza checksum per autenticare le applicazioni** nella scheda di configurazione **Generale**).

Se si desidera consentire l'accesso alla rete da parte dell'applicazione, è necessario aggiungere il suo checksum (un identificativo univoco) alla lista di checksum riconosciuti.

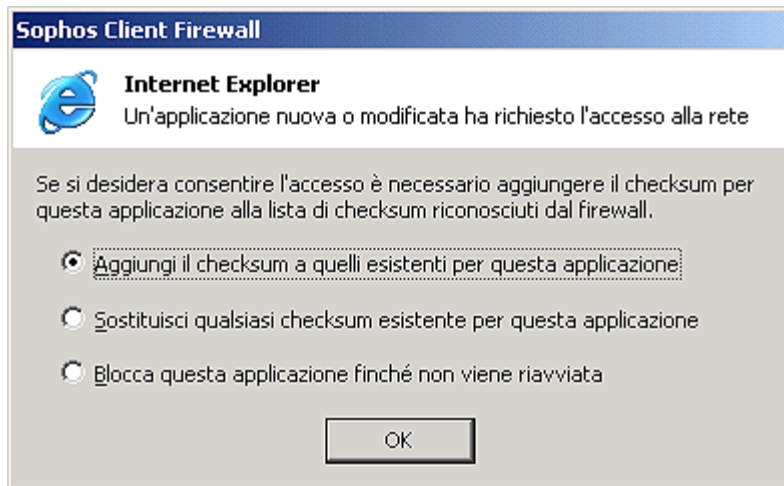
Selezionare una delle seguenti opzioni:

Aggiungi il checksum a quelli esistenti per questa applicazione consente molteplici versioni di questa applicazione.

Sostituisci qualsiasi checksum esistente per questa applicazione sostituisce tutti i checksum esistenti per l'applicazione con quello che richiede l'accesso, consentendo pertanto solo la versione più recente dell'applicazione stessa.

Blocca questa applicazione finché non viene riavviata blocca l'applicazione in questa specifica occasione. Questa è l'opzione predefinita e sarà selezionata anche premendo il tasto Esc.

Al termine dell'operazione, cliccare su OK.

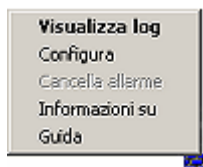


5 Utilizzo del visualizzatore del log

Utilizzo del visualizzatore del log

È possibile utilizzare il visualizzatore del log per vedere i record del traffico consentito e bloccato, oltre che come log di sistema.

Per accedere al log di sistema, cliccare con il tasto destro del mouse sull'icona del firewall posta nell'area di notifica e selezionare **Visualizza log**:



Questa sezione descrive le principali impostazioni del visualizzatore del log.

- [Introduzione al visualizzatore del log](#)
- [Connessioni bloccate](#)

- Connessioni consentite
- Processi
- Log di sistema

Introduzione al visualizzatore del log

Il visualizzatore del log consente di visualizzare i dettagli del database degli eventi, tra i quali le connessioni che sono state consentite o bloccate, il log di sistema e tutti gli allarmi generati.

Il visualizzatore del log si divide in due riquadri. Il riquadro di sinistra mostra un menu ad albero nel quale è possibile selezionare schermate differenti, mentre il riquadro di destra contiene un elenco delle informazioni rilevanti registrate per una specifica schermata. Le informazioni comprendono:

- Connessioni bloccate
- Connessioni consentite
- Processi
- Log di sistema

È possibile anche personalizzare il layout della schermata, ordinare i dati visualizzati ed esportare i dati in un file. Le opzioni di personalizzazione includono:

- Filtro delle voci di log
- Aggiunta/Rimozione delle colonne
- Personalizzazione del formato dei dati
- Personalizzazione del layout della schermata

Connessioni bloccate

Il visualizzatore del log consente di visualizzare i dettagli del database degli eventi. Questa schermata elenca le connessioni che sono state bloccate. La data e l'ora relative al tentativo di connessione sono visualizzate nel campo **Ora di inizio**. Riguardo alle connessioni odierne bloccate, è visualizzata soltanto l'ora. I campi **Uptime**, **Velocità dati**, **Inviati** e **Ricevuti** visualizzano i dati dopo la chiusura della connessione.

In alcuni casi, è possibile che il log mostri una connessione bloccata recante un messaggio come 'Modalità apprendimento' nel campo **Ragione**. In questo caso, viene richiesto contemporaneamente di configurare la corrispondente finestra di dialogo Apprendimento. Il messaggio cambierà a seconda delle scelte effettuate. Se si consente la connessione, l'intera voce viene spostata nella pagina delle Connessioni

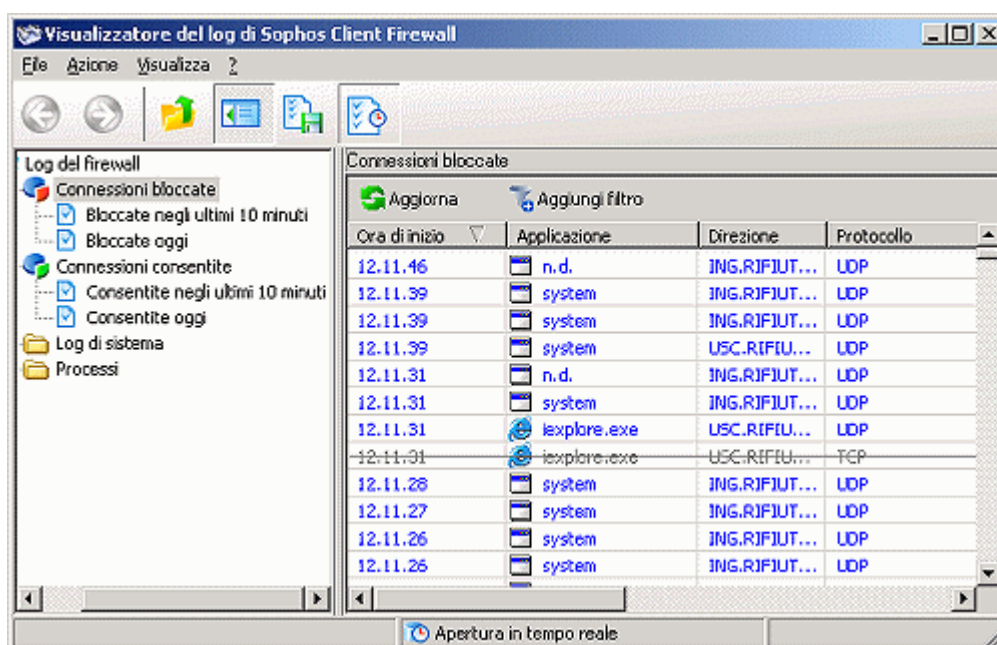
consentite e la voce è visualizzata in grigio, attraversata da una linea.

Cliccando sul relativo nodo, è possibile anche vedere:

- le applicazioni bloccate negli ultimi 10 minuti
- le applicazioni bloccate oggi.

Per gestire ulteriormente i dati sono possibili le seguenti operazioni:

- Filtro delle voci di log
- Aggiunta/Rimozione delle colonne
- Personalizzazione del formato dei dati
- Personalizzazione del layout della schermata



Connessioni consentite

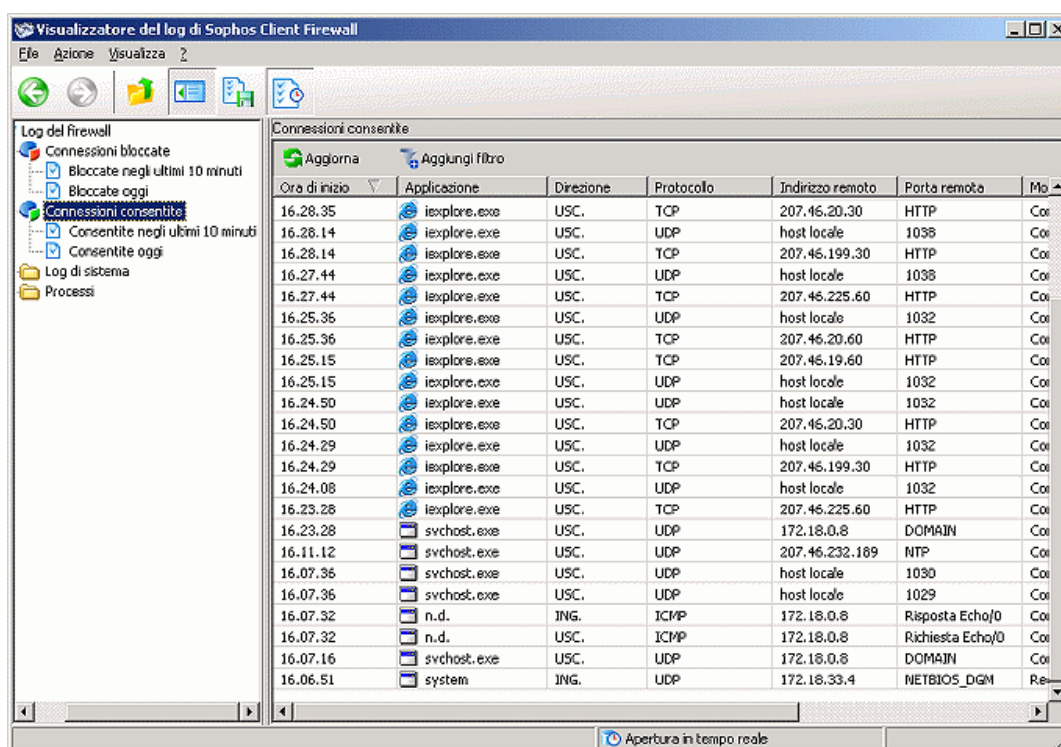
Il visualizzatore del log consente di visualizzare i dettagli del database degli eventi. Questa schermata elenca le connessioni che sono state consentite. La data e l'ora relative al tentativo di connessione sono visualizzate nel campo **Ora di inizio**. Riguardo alle connessioni odierne, è visualizzata soltanto l'ora. I campi **Uptime**, **Velocità dati**, **Inviati** e **Ricevuti** visualizzano i dati dopo la chiusura della connessione.

Cliccando sul relativo nodo, è possibile anche vedere:

- le connessioni consentite negli ultimi 10 minuti
- le connessioni consentite oggi

Per gestire ulteriormente i dati sono possibili le seguenti operazioni:

- Aggiunta/Rimozione delle colonne
- Personalizzazione del formato dei dati
- Personalizzazione del layout della schermata

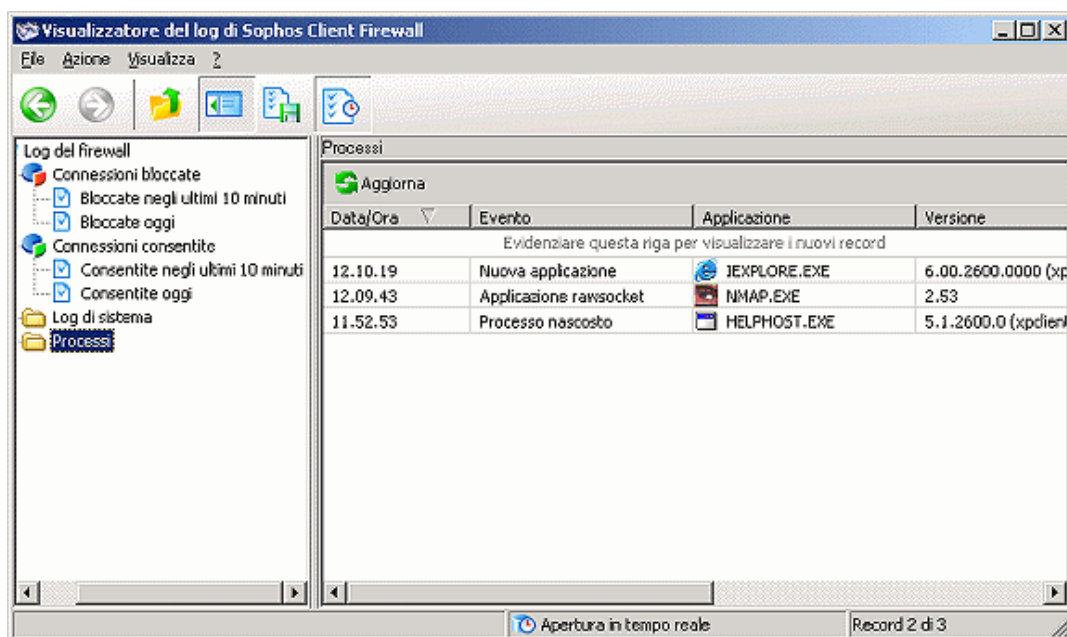


Processi

Il visualizzatore del log consente di visualizzare i dettagli del database degli eventi. Da questa pagina vengono gestiti processi e checksum. Riguardo alle connessioni odierne, è visualizzata soltanto l'ora nel campo Data/Ora.

Per gestire ulteriormente i dati sono possibili le seguenti operazioni:

- Aggiunta/Rimozione delle colonne
- Personalizzazione del formato dei dati
- Personalizzazione del layout della schermata

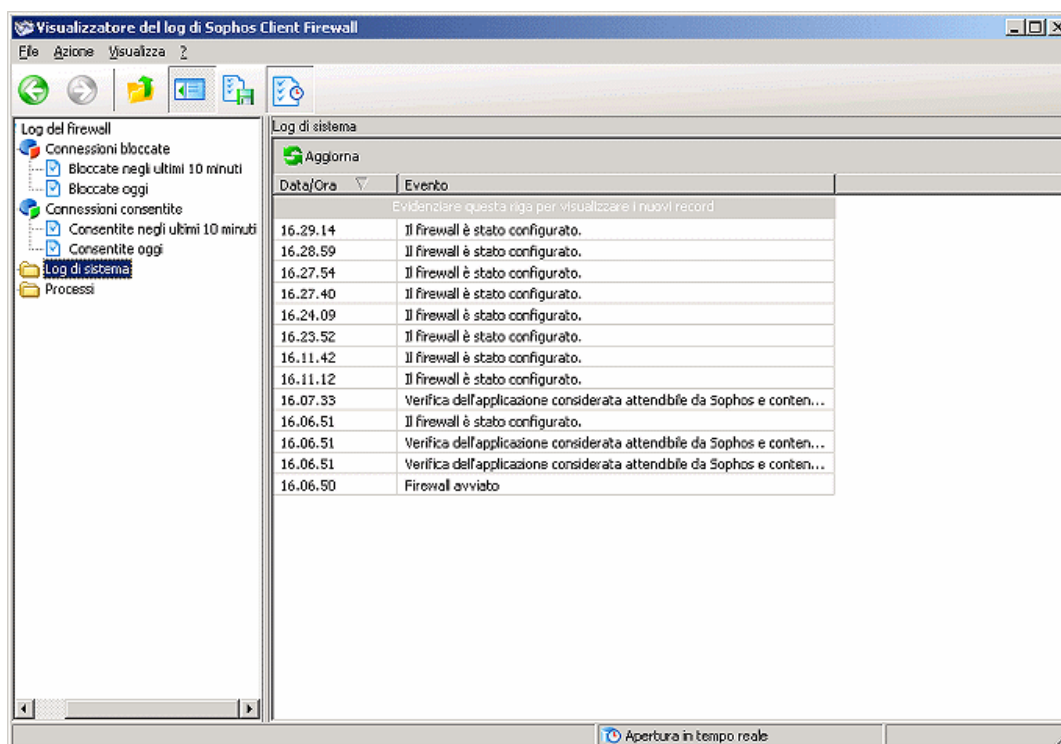


Log di sistema

Il log di sistema consente di visualizzare l'attività della rete registrata durante un certo arco di tempo. Per impostazione predefinita la schermata mostra i campi **Data/Ora** ed **Evento**. Riguardo alle connessioni odierne, è visualizzata soltanto l'ora.

Per gestire ulteriormente i dati sono possibili le seguenti operazioni:

- Aggiunta/Rimozione delle colonne
- Personalizzazione del formato dei dati
- Personalizzazione del layout della schermata



6 Glossario

Glossario

Cliccare su uno dei collegamenti seguenti per leggere la definizione.

- [Checksum](#)
- [NetBIOS](#)
- [Processo nascosto](#)
- [Protocollo di rete](#)
- [Raw socket](#)
- [Regole delle applicazioni](#)
- [Regole globali](#)
- [Traffico ICMP](#)

Indice

A

attivazione: del firewall 11

B

browser: consenso 6

C

checksum: consenso 22

condivisione file e stampanti:
consenso 8

configurazione: firewall 12

configurazioni: importazione 24

D

disattivazione: del firewall 11

download FTP: consenso 16

E

e-mail: consenso 7

G

glossario: panoramica 39

I

icona nell'area di notifica 5

interfaccia: panoramica 5

introduzione: panoramica 4

introduzione: per iniziare 4

L

log 26

log di sistema: panoramica 38

log: configurazione 27

M

modalità interattiva: applicazioni 31

modalità interattiva: checksum 33

modalità interattiva: impostazione 9

modalità interattiva: panoramica 28

modalità interattiva: processi nascosti
29

modalità interattiva: raw socket 32

modalità interattiva: regole globali 30

modalità interattiva: selezione 12

modalità non interattiva: selezione 12

P

panoramica: configurazione 12

priorità regole 25

processi nascosti: consenso 19

R

- raw socket: consenso 21
- regole applicazioni: impostazione 18
- regole globali: impostazione 17
- regole: priorità 25
- reportistica 26
- reportistica: centrale 26

T

- traffico ICMP 13
- traffico LAN: consenso 14

V

- visualizzatore del log: connessioni bloccate 35
- visualizzatore del log: connessioni consentite 36
- visualizzatore del log: introduzione 35
- visualizzatore del log: panoramica 34
- visualizzatore del log: processi 37