Manuale d'uso di eXtensiveControl®

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Manuale d'uso di eXtensiveControl

Aprile 2010

Informazioni di servizio e di supporto

Versione del prodotto

Questo manuale si riferisce al programma eXtensiveControl® versione 2.x. Per ottenere supporto tecnico, servizi per l'utente e informazioni sulla vendita del prodotto è possibile utilizzare l'indirizzo riportato in seguito.

Telefono

Supporto tecnico e commerciale:

+39 (0)521 708811

WEB

http://www.symbolic.it

Posta elettronica

Supporto tecnico: <support@symbolic.it>

Vendite: <sales@symbolic.it>

Indirizzo di posta

Symbolic S.p.A.
Viale Mentana, 29
CAP 43121 Parma
Italy

Orari di assistenza del prodotto

Il supporto telefonico è fornito nei giorni feriali dalle 8:30 alle 12:30 e dalle 14:30 alle 18:30 (ora locale)

È necessario un contratto di supporto.

Capitolo 1. Introduzione ad eXtensiveControl®

La homepage di eXtensiveControl®

Per collegarsi alla homepage è possibile lanciare il browser sulla macchina in cui è installato eXtensiveControl® e digitare l'indirizzo e la porta su cui il configuratore è in ascolto. Per default tale indirizzo è il localhost (127.0.0.1) e la porta la 8000, ma è possibile che durante l'installazione l'amministratore abbia cambiato la porta (se ad esempio questa è già impegnata da un altro processo). In questo caso bisognerà utilizzare i valori appropriati. Per essere sicuri di raggiungere il configuratore indipendentemente dall'indirizzo e dalla porta utilizzata è possibile utilizzare il link all'interno del menu *programmi* del sistema operativo.

Una possibile stringa da digitare nella barra degli URL del browser sarà dunque:

http://127.0.0.1:8000

Una volta raggiunto il configuratore, verrà presentata la schermata principale da cui sarà possibile accedere alle 3 sezioni del programma:

- *Inserimento spam*: consente agli utenti autorizzati di accedere alla sezione di uploading delle mail. Per maggiori informazioni vedere Capitolo 22, *Inserimento Spam*
- *Wizard di configurazione*: consente una configurazione rapida per utenti inesperti o che hanno appena preso visione del prodotto. Per ulteriori dettagli vedere: Capitolo 4, *Wizard di configurazione*
- *Configuratore*: trattasi della console principale con cui l'amministratore gestisce la maggior parte delle funzioni del prodotto. Per ulteriori dettagli vedere la sezione chiamata «Il configuratore»

Il configuratore

Il configuratore rappresenta il centro di controllo per amministrare la quasi totalità delle funzioni di eXtensiveControl®. Con esso l'amministratore può ad esempio definire le policy che gestiscono i diritti degli utenti o compilare i report per avere informazioni su quello che accade nella rete locale.

Il prodotto consta di tre moduli principali che vengono utilizzati per supportare le policy aziendali. Il modulo WEB può essere impiegato per limitare la navigazione degli utenti in base alla fascia oraria, alla tipologia dei siti o ad altri parametri. Se si desiderano informazioni a riguardo vedere Capitolo 6, *Modulo WEB*.

I moduli POP3 e SMTP vengono invece utilizzati per ricevere e spedire posta e al tempo stesso imporre vincoli quali ad esempio filtri antivirus, antispam, antiphishing e regole sul contenuto del messaggio. Se si desiderano informazioni a riguardo vedere Capitolo 7, *Funzionamento del modulo POP3* e Capitolo 10, *Funzionamento del modulo SMTP*.

Il configuratore è diviso in varie sezioni:

- *Moduli*: la sezione moduli consente di accedere alla stato e alla configurazione dei tre moduli principali (WEB, POP3 ed SMTP).
- *Sistema*: la sezione sistema consente di accedere allo stato e alla configurazione dei due processi secondari: il Message Transfer Agent (MTA) (vedere Capitolo 17, *MTA*) e la cache DNS (Littlename) (vedere Capitolo 16, *DNS*). Inoltre attraverso la sezione Sistema è anche possibile collegare il prodotto ad un dominio Windows 2000/2003 (supporto Active Directory), accedere alle opzioni relative al database personalizzato dall'utente, al motore antispam, alle modalità di aggiornamento dei database e alla sezione di licensing del prodotto (vedere Capitolo 19, *Sistema*)s.
- *Report*: la sezione di reportistica consente di compilare report basandosi sui file di log che il sistema accumula nel tempo e che contengono gli accessi che gli utenti fanno ai moduli. In questo modo

l'amministratore può prendere visione dell'attività degli utenti sulla rete, ad esempio i messaggi che ricevono, i siti che visitano, la quantità di banda impegnata, ecc. Per ulteriori informazioni vedere Capitolo 20, *Report*

- *Configuratore*: la sezione "Configuratore" consente di modificare le impostazioni relative al configuratore stesso, per esempio da esso è possibile cambiare l'indirizzo e la porta su cui il configuratore riceve le connessioni, cambiare la password di amministratore, impostare i diritti di accesso, ecc. In più è possibile definire quali utenti possono collegarsi al configuratore stesso e alla sezione di "Inserimento Spam". Vedere Capitolo 21, *Configuratore* per i dettagli.

In qualunque momento è possibile utilizzare il tasto Home, in alto a sinistra, per tornare al menu principale.

Capitolo 2. Guida rapida

Installazione

Per installare il prodotto lanciare il programma di setup che si trova sul CD−ROM o che è stato scaricato dal web.

Una volta avviato, il setup mostrerà lo schermo di benvenuto e la doppia schermata delle licenze.

Viene a questo punto presentata una finestra di dialogo ove è possibile inserire il codice per l'attivazione di eXtensiveControl e del plug−in SurfControl per la categorizzazione dei siti. Se viene lasciata la scritta "<*prova*>", il rispettivo elemento verrà abilitato in modalità *trial* con una durata di 30 giorni dalla data di installazione.

A questo punto è richiesto il percorso in cui installare il prodotto. Se si desidera installare il prodotto in una cartella differente da quella presentata, fare click sul tasto ***Sfoglia***. Fare quindi click sul pulsante ***Avanti*** per procedere.

Selezionare sotto quale voce del menu *Programmi* dovrà essere impostato il link per accedere al configuratore e quindi fare click sul pulsante ***Avanti*** per procedere.

Viene creata la struttura delle directory e vengono copiati i file.

Viene quindi chiesto se si desidera lanciare automaticamente il configuratore ad ogni avvio del sistema. Se non ci sono particolari motivi per scegliere altrimenti, rispondere affermativamente selezionando il tasto ***Yes***. Se si sceglie di non avviare automaticamente il configuratore, sarà necessario farlo manualmente agendo sul servizio *cf_conf* dal pannello di controllo, attraverso il *Service Manager* di Windows. Quando il configuratore non è avviato, non è possibile utilizzare il browser per modificare le impostazioni di eXtensiveControl® e occorre intervenire manualmente sui file di configurazione.

Si ha a questo punto l'opportunità di specificare una porta su cui il configuratore si porrà in ascolto (l'indirizzo per default è *localhost*, cioè 127.0.0.1). Se non si hanno già altre applicazioni in ascolto, lasciare il valore di default, cioè la porta 8000, altrimenti spuntare la casella e inserire un altro valore.

Digitare quindi una password di almeno otto caratteri che sarà associata all'utente Admin. Tale utente verrà utilizzato successivamente quando si accederà al configuratore via web.

Al termine dell'installazione verrà automaticamente lanciato il browser che si aprirà nella pagina del wizard. Se ci dovessero essere problemi di visualizzazione attendere alcuni istanti e quindi richiedere un reload della pagina. Nel caso il problema persista provare un collegamento diretto con l'URL *http://127.0.0.1:8000* (o altra porta se non si è utilizzato quella di default).

Aggiornamenti

Gli aggiornamenti possono essere effettuati seguendo la stessa procedura descritta sopra per l'installazione del prodotto.

A differenza dell'installazione, alla fine della fase di aggiornamento verrà chiesto se si desidera riavviare il sistema. È infatti necessario un riavvio per far sì che i moduli vengano aggiornati ed il prodotto torni ad essere operativo.

Il Wizard

Al termine dell'installazione viene avviato il servizio *cf_conf* che funziona da server web e consentirà all'amministratore di configurare il prodotto attraverso un browser.

Il configuratore per default ascolta sulla porta 8000 del localhost (cioè l'indirizzo IP 127.0.0.1). La porta può essere cambiata durante l'installazione. L'indirizzo invece dovrà essere cambiato attraverso l'interfaccia web una volta terminata l'installazione se si desidera poter configurare il prodotto anche da macchine diverse da quella su cui è installato (è necessario modificare anche la lista di indirizzi IP relativa alle macchine che possono connettersi per usufruire del servizio di accesso remoto).

È disponibile un help in linea a cui è possibile accedere facendo un clic sull'icona azzurra con il punto di domanda in alto a destra.

In alternativa è possibile accedere direttamente al manuale, in formato HTML o pdf, nelle cartelle *docs/html* e *docs/pdf* oppure dai link ad essi relativi dal menu Programmi.

Se si installa il prodotto su Windows 2003 Server potrebbe essere necessario intervenire sulla configurazione di Internet Explorer, quest'ultimo per default è configurato in modo restrittivo e può bloccare le pagine servite dal configuratore. Se si presenta questo problema selezionare, da Internet Explorer, la voce Strumenti, Opzioni Internet e quindi il tab Protezione e aggiungere localhost (127.0.0.1) o l'indirizzo IP della vostra macchina (se avete deciso di rendere il prodotto disponibile per una configurazione da remoto) nella lista dei siti attendibili.

Si raccomanda di riferirsi alla sezione di help contestuale o al manuale una volta installato il prodotto, per avere informazioni su come configurarlo e renderlo operativo.

Capitolo 3. Requisiti di sistema

I requisiti minimi per l'installazione di eXtensiveControl® sono i seguenti:

- Windows 2000, Windows XP, Windows 2003 Server.
- per la configurazione attraverso l'interfaccia Web è richiesto Internet Explorer.
- Processore x86 compatibile (Intel, AMD, ecc.) 1GHz o superiore
- 200 MB di spazio libero su disco, utilizzando il Plug−in di SurfControl® la richiesta minima è 400 MB di spazio
- 512 Mb di memoria RAM. Può essere necessaria ancora più RAM se si fanno funzionare altre applicazioni sulla stessa macchina.

I requisiti sopra indicati rappresentano dei valori minimi. I requisiti come potenza di calcolo e memoria da utilizzare dipendono dal numero di utenti e dai servizi richiesti. In particolare l'uso del controllo antivirus sulla posta elettronica potrebbe richiedere requisiti superiori in base al traffico e al tipo di messaggi (messaggi di grandi dimensioni richiedono un maggiore quantitativo di memori). Per eventuali dubbi è possibile consultare il supporto tecnico (come indicato ne Informazioni di servizio e di supporto) per ottenere maggiori

informazioni.

eXtensiveControl® tiene traccia del traffico che lo attraversa mediante i file di log. Lo spazio occupato da tali file dipende essenzialmente dal numero di servizi attivi e dalla quantità di traffico che gestiscono. Un limitato spazio su disco renderà necessario ripulire più di frequente la directory contenente i file di log ed eventualmente archiviare questi ultimi, per mantenere sempre il sistema in condizioni operative eccellenti.

Capitolo 4. Wizard di configurazione

Il Wizard di configurazione può essere utilizzato per configurare le funzionalita base di eXtensiveControl® dopo l'installazione. Le opzioni avanzate potranno essere attivate successivamente dal configuratore classico.

Vi sono tre modi di utilizzo del prodotto, elencati in ordine crescente di complessità:

- *Wizard*: prima configurazione dopo l'installazione e per configurazioni semplici (procedura passo passo secondo uno schema predefinito).
- *Configuratore*: è la modalità tipica che l'amministratore adotta quando deve cambiare le impostazioni del prodotto. A differenza del Wizard, quasi tutte le opzioni sono facilmente disponibili. Non vi sono linee guida da seguire.
- *Modifica dei file di configurazione*: si tratta della soluzione più avanzata e flessibile, ma è anche la più complessa da gestire. L'utente ha la possibilità, modificando manualmente i file di configurazione, di accedere a tutte le opzioni.

Il Wizard di configurazione è suddiviso in fasi successive che accompagnano l'amministratore durante la fase di configurazione.

Schermata iniziale

La schermata iniziale è un semplice benvenuto al wizard di configurazione. Fare clic sul tasto Avanti per proseguire.

Collegamento con un dominio Active Directory

Il primo passo per configurare il prodotto con il Wizard consiste nel decidere se si desidera collegare eXtensiveControl® ad un dominio Active Directory (Windows 2000 o Windows 2003). Attraverso Active Directory sarà possibile usufruire del servizio di autenticazione sul dominio per quanto riguarda la navigazione web. Inoltre, se si utilizza un server Exchange integrato nel dominio, sarà possibile usufruire di un filtro sulla posta atto a respingere le mail indirizzate ad utenti non esistenti.

Per collegare eXtensiveControl® ad Active Directory è necessario fornire il nome del dominio a cui si desidera collegarsi (es. "example.com") e le credenziali di un utente di dominio avente il diritto di effettuare le query sul domain controller.

Normalmente queste informazioni sono sufficienti per permettere al prodotto di effettuare all'occorrenza il collegamento ad Active Directory. In alcuni casi tuttavia può essere necessario fornire il nome o l'indirizzo IP di uno dei domain controller appartenente al dominio specificato (il prodotto effettua un primo test con i dati forniti e poi richiederà espressamente questo terzo parametro nel caso non sia in grado di acquisirlo autonomamente).

Se si desiderano ulteriori informazioni sull'interazione di eXtensiveControl® con un dominio Active Directory, vedere Capitolo 15, *Collegamento ad Active Directory*.

Configurazione del Modulo WEB

Attraverso questa sezione è possibile abilitare gli utenti alla navigazione attraverso il modulo Web. Se tale modulo viene attivato, sarà necessario impostare un indirizzo di ascolto e relativa porta su cui il modulo accetterà le connessioni dei client. Ricordarsi che per abilitare i client ad utilizzare il modulo WEB è necessario impostare l'uso del proxy nei browser. Se si utilizza Internet Explorer tale impostazione si trova nel menu Strumenti/Opzioni Internet/ Connessioni/Impostazioni LAN. Nella sezione Server Proxy occorre digitare lo stesso indirizzo su cui il modulo viene messo in ascolto.

È possibile abilitare la categorizzazione dei siti attraverso la relativa checkbox. Se tale impostazione viene attivata, verrà presentata una lista di categorie. Selezionandole sarà possibile escludere gli utenti dalla navigazione verso siti appartenenti a tali categorie. Per default il wizard imposterà l'utilizzo del database BluePrint Data®. In caso si intenda utilizzare il database WebSense/Surfcontrol è possibile – una volta terminato il wizard – modificare l'impostazione attraverso il menù *Sistema/Categorizzatore Web/Avanzate* del configuratore.

Per ulteriori informazioni sui parametri di configurazione del modulo WEB vedere Capitolo 6, *Modulo WEB*, se invece si desidera una panoramica generale sulle funzioni svolte dal modulo WEB vedere Capitolo 5, *Funzionamento del modulo WEB*.

Configurazione del Modulo POP3

Il modulo POP3 gestisce la ricezione della posta attraverso l'omonimo protocollo ed è in grado di effettuare un controllo antivirus, antispam ed antiphishing sui messaggi in arrivo. Una volta abilitato questo modulo è necessario fornire un indirizzo e una porta sui quali il modulo accetterà le connessioni ed ai quali i client si collegheranno per scaricare la posta. È possibile inoltre definire un default server verso il quale il proxy si collegherà (quando riceverà una richiesta dai client) per scaricare la posta.

Durante il passaggio dei messaggi possono essere applicati vari filtri fra i quali quali il controllo antivirus, antispam ed antiphishing.

Il modulo POP3 viene tipicamente utilizzato quando la rete non è dotata di un server di posta interno ed è pertanto necessario controllare la posta durante il download da un server esterno. Qualora la rete sia dotata di un server di posta interno è preferibile l'utilizzo del modulo SMTP.

Per avere maggiori informazioni sul funzionamento generale del modulo POP3, vedere Capitolo 7, *Funzionamento del modulo POP3*, se invece si desidera avere un aiuto sul significato dei parametri per la configurazione vedere Capitolo 8, *Modulo POP3*.

Configurazione del modulo SMTP

Il modulo SMTP gestisce la ricezione della posta attraverso l'omonimo protocollo ed è in grado di effettuare il controllo antivirus, antispam ed antiphishing sui messaggi in transito. Una volta abilitato questo modulo è necessario fornire un indirizzo e una porta sui quali il modulo accetterà le connessioni ed ai quali i client si collegano per spedire la posta.

Durante il passaggio dei messaggi possono essere applicati vari filtri fra i quali il controllo antivirus, antispam, antiphishing ed il filtro di reject delle mail se si utilizza un server Exchange (attivabile solo se è stato scelto di collegare eXtensiveControl® ad un dominio Active Directory).

Il modulo SMTP viene tipicamente utilizzato quando la rete è dotata di un server interno. Per utilizzare il modulo SMTP *è necessario abilitare* anche il modulo MTA per la spedizione dei messaggi (vedere la sezione chiamata «Configurazione del Modulo MTA»), in quanto il modulo SMTP si occupa solo della ricezione dei

messaggi di posta ma non di effettuare la spedizione (compito assegnato allo MTA).

Per avere maggiori informazioni sul funzionamento generale del modulo SMTP vedere Capitolo 10, *Funzionamento del modulo SMTP*; se invece si desidera avere un aiuto sul significato dei parametri per la configurazione vedere Capitolo 11, *Modulo SMTP*.

Configurazione del Modulo MTA

Il modulo MTA viene utilizzato per spedire i messaggi ricevuti dal modulo SMTP verso un server interno o esterno di relay. Tale modulo è indipendente dal modulo SMTP, poiché lo MTA ha anche il compito di inviare eventuali notifiche all'amministratore (o in generale messaggi creati da eXtensiveControl®) e di inviare mail mail "rilasciate" dalla quarantena. Pertanto il modulo dovrebbe essere configurato anche se il modulo SMTP non è stato attivato.

È possibile scegliere il server di destinazione di un messaggio in base al dominio del destinatario dello stesso.

Per avere ulteriori informazioni sul funzionamento del MTA vedere Capitolo 17, *MTA*.

Aggiornamenti

La sezione permette di pianificare il download del database web, di spam e di phishing dai server di Intrinsic (o SurfControl® nel caso dell'omonimo database) al fine di mantenere eXtensiveControl® sempre aggiornato e ottenere un rating elevato nella funzionalità di filtro dei contenuti.

Spuntando il checkbox "Vuoi abilitare l'aggiornamento automatico del database web?" è possibile definire la pianificazione dell'aggiornamento del database web. Si può definire l'orario di esecuzione e la frequenza, giornaliera o settimanale e in quest'ultima ipotesi i giorni della settimana in cui attivare l'operazione. Analogo il caso per gli altri database.

Se si sceglie la periodicità di esecuzione settimanale è necessario selezionare almeno un giorno della settimana.

Fine

In questa sezione sono riportati tutti i dati inseriti precedentemente nel wizard di configurazione. Premendo Finito, si salva la configurazione su disco e si avviano i moduli abilitati. Il Wizard di configurazione, creando una nuova configurazione, cancella eventuali configurazioni preesistenti.

Come già anticipato nella sezione WEB, se per rendere operativa la configurazione è necessario installare/scaricare alcuni database, verrà presentata una schermata dove sarà possibile effettuare tale operazione. Nel caso sia necessario utilizzare un proxy per accedere alla rete esterna, sarà possibile fornire in tale schermata i parametri necessari.

In particolare le opzioni presenti sono:

- *Scarica ora*: fa si che il wizard scarichi attraverso una connessione http i database di cui ha bisogno. Se per accedere all'esterno si utilizza un server proxy (HTTP), è possibile specificare nei box sotto l'indirizzo IP del proxy, la porta di ascolto ed eventuali credenziali per effettuare il collegamento al proxy).
- *Aggiorna da CD*: installa i database necessari dal CD di eXtensiveControl®. Se il CD non dovesse essere disponibile, l'operazione riporterà un errore e consentirà all'utente di specificare manualmente un percorso ove reperire i dati necessari.

> È importante rilevare che l'operazione di installazione dei database da CD non consiste in una semplice copia di uno o più file sul disco fisso, ma necessita, per essere portata a termine correttamente, anche dell'aggiornamento di alcuni file di configurazione. Evitare dunque di copiare manualmente file da CD ed utilizzare la procedura del wizard.
>
> Si ricorda inoltre che il CD contiene database quasi certamente meno recenti di quelli disponibili sul WEB, pertanto si consiglia di pianificare un aggiornamento periodico per mantenere elevata l'efficienza del prodotto.

Se si fa clic sul tasto *Continua* invece si sceglie di non procedere immediatamente all'aggiornamento e di provvedere manualmente in seguito a tale operazione. Naturalmente alcuni proxy potrebbero non operare correttamente fino a quando i database non vengono aggiornati. In particolare il servizio di categorizzazione web (cf_catmanager) non può categorizzare i siti col database di surfcontrol se questo non viene installato. Se si verifica questo tipo di errore, il servizio non parte e riporta il problema nei file di debug (visualizzatore log).

Capitolo 5. Funzionamento del modulo WEB

Introduzione

Il modulo WEB viene utilizzato per regolamentare l'accesso al Worl Wide Web da parte degli utenti. Esempio di utilizzo possono essere:

- Impedire a determinate macchine di navigare.
- Impedire a tutti o a parte degli utenti di raggiungere siti con un dato contenuto (es. pornografia, violenza, sport, notizie, motori di ricerca, ecc.)
- Impedire la navigazione di tutti o parte degli utenti in determinate fasce orarie.
- Autenticare la navigazione degli utenti in modo che sia nota l'identità di chi visita determinati siti.

Queste regole possono essere impostate tramite l'uso delle regole di accesso (ACL). Per maggiori informazioni vedere la sezione chiamata «Regole di accesso».

Configurazione del modulo WEB

La configurazione base del modulo WEB è semplice in quanto occorre definire un server con un indirizzo di ascolto (raggiungibile dai client della rete) e configurare i browser dei vari client affinchè utilizzino il modulo come proxy.

È opportuno verificare, nel caso si desideri utilizzare il categorizzatore di SurfControl®, che questo sia installato e attivato prima di avviare il proxy. L'installazione può essere fatta sia dal Wizard sia dalla sezione Categorizzatore Web (all'interno della sezione Sistema). Il Wizard è in grado di effettuare l'installazione del database sia da CD (se disponibile) che tramite download dal Web. Dalla sezione Categorizzazione Web invece è possibile solo il download.

Se si dispone di un firewall perimetrale è inoltre consigliabile impostare su quest'ultimo una regola tale da consentire l'accesso al web solo alla macchina su cui è installato eXtensiveControl® in modo da evitare che gli utenti aggirino il modulo WEB di eXtensiveControl® e si liberino da ogni policy aziendale semplicemente modificando le impostazioni dei propri browser.

Per abilitare l'uso del modulo WEB in Internet Explorer occorre accedere al menù Strumenti/ Opzioni Internet/ Connessioni/ Impostazioni LAN e inserire l'indirizzo del modulo WEB. Può inoltre essere utile spuntare la casella Ignora server proxy per indirizzi locali in modo da evitare l'uso del proxy quando si accede ad eventuali server Web interni.

Capitolo 6. Modulo WEB

Il modulo WEB viene utilizzato per consentire agli utenti di navigare e allo stesso tempo per imporre loro eventuali politiche restrittive. Se si desidera un'introduzione al funzionamento del modulo WEB vedere Capitolo 5, *Funzionamento del modulo WEB*.

Info

La sezione Info presenta un riepilogo dello stato del modulo:

- Stato: Lo stato del modulo può essere: Disabilitato, Fermo, Avviato o In avvio.
- Data di avvio: Ultima volta che il modulo è stato avviato.
- Dimensioni file di log: Spazio occupato su disco dal file di log (estensione .log).
- Dimensioni file comandi processati: Spazio occupato su disco dal file comandi (estensione .lcd).
- Dimensioni file di debug: Spazio occupato su disco dal file con le informazioni di debug (estensione .err).

Ogni modulo, quando avviato, registra le informazioni relative al proprio funzionamento su tre file che portano il nome del modulo stesso ed estensioni (.log, .lcd e .err) dipendenti dal tipo di dati che raccolgono. Ogni giorno, ad un orario stabilito (che può essere variato a piacere) i file vengono rinominati e viene aggiunta la data corrente nel nome del file e poi viene creato un nuovo file senza data per il nuovo giorno. In questo modo i file si accumulano giorno per giorno e possono essere facilmente identificati dalla data che hanno nel nome stesso. Per default la rotazione avviene alle 23.58, quindi il file rinominato avrà la data corrente e tutte le informazioni relative a quel giorno (almeno fino alle 23:58) e gli ultimi 2 minuti del giorno precedente. In questo modo si otterranno dei file con riportata nel nome una data e all'interno di essi tutti i log relativi alla data indicata nel nome.

Nella parte inferiore della sezione è possibile accedere alle statistiche del modulo nell'ultima ora, giorno e settimana. Viene fornito un riassunto grafico delle attività del modulo, in modo da riconoscere immediatamente eventuali picchi di traffico, oltre al valore minimo, massimo e medio dell'attività visualizzata. "Tipo" specifica la caratteristica del modulo che si vuole visualizzare e "Intervallo" l'intervallo temporale che si desidera considerare nella statistica. "Visualizza statistiche" mostra le statistiche desiderate.

Avanzate

Significato dei parametri disponibili:

- Durata massima di una connessione: durata massima in secondi di una connessione. Un valore pari a 0 indica un tempo infinito.
- Durata massima di una connessione inattiva: tempo massimo in secondi dopo il quale una connessione viene terminata se non vengono ricevuti dei dati.
- Livello di debug: regola la quantità di informazioni che viene generata dal modulo e salvata nel file di debug (estensione .err). Più piccolo è tale valore, minori sono le informazioni registrate. Tipicamente si incrementa il livello di debug in fase di diagnostica per determinare la causa di eventuali problemi.
- Consenti host per cui non esiste il nome: può capitare che eXtensiveControl® debba eseguire una query DNS inversa da indirizzo IP a nome per applicare la politica di accesso definita nella sezione "Regole di accesso". Questo accade ad esempio se si imposta una politica basata sui nomi delle macchine piuttosto che sui loro indirizzi IP. Se la conversione fallisce la connessione viene rifiutata a meno che questo flag non venga impostato.
- Utilizza il Server Proxy: consente di collegare eXtensiveControl® in cascata un altro server proxy. Viene solitamente impiegato quando per accedere alla rete esterna bisogna passare per un altro proxy HTTP.
- Username per il Server Proxy: nome utente utilizzato per l'autenticazione al Server Proxy.

- Password per il Server Proxy: password utilizzata per l'autenticazione al Server Proxy.
- Tempo di cache per autenticazione utente: Quando nelle regole di accesso si abilita l'autenticazione utente, viene creata un'associazione computer/utente in modo che eventuali richieste provenienti da un host siano considerate come effettuate dall'utente che ha effettuato la prima autenticazione. Questo funzionamento permette di utilizzare anche applicazioni che non supportano l'accesso tramite proxy con richiesta di autenticazione e inoltre evita che l'utente debba inserire username e password ogni volta che esegue un nuovo programma che utilizza il proxy Web. L'associazione computer/utente viene mantenuta per il tempo indicato da questo parametro. Il valore 0 disabilita l'associazione computer/utente.
- Estensioni proibite: vengono negati i download dei file aventi le estensioni elencate nel relativo box. Le estensioni vengono inserite senza wildcard e sono separate da uno spazio (es. *zip rar exe com*).
- Blocca i siti non categorizzati (sconosciuti): se è abilitata la categorizzazione degli URL e un sito non è presente nel database prescelto, l'accesso è controllato dal valore di questo flag.

Dopo avere cambiato la configurazione per salvare le modifiche è necessario premere il pulsante "Salva". Il pulsante "Annulla le modifiche" effettua una rilettura della configurazione presente su disco cancellando così le modifiche inserite e non ancora salvate.

Dalla versione 1.2 il prodotto è dotato di un servizio a parte chiamato *cf_catmanager* con il quale il modulo WEB si interfaccia per gestire la categorizzazione dei siti. Operativamente questo significa che la gestione dei database Symbolic, BluePrint Data® e SurfControl®, nonchè la pianificiazione degli aggiornamenti avverrà in una sezione a parte chiamata Categorizzatore Web (nel menu Sistema) e non più nella sezione Avanzate del proxy HTTP. Per ulteriori informazioni vedere: la sezione chiamata «Categorizzazione WEB»

Server

I server vengono utilizzati per associare ad un dato modulo uno o più indirizzi e porte di ascolto. Quando un client deve utilizzare un modulo per accedere ad un dato servizio deve infatti conoscere l'indirizzo e la porta TCP a cui connettersi per inviare le richieste. Tali parametri vengono configurati in questa sezione e sono specifici per ogni modulo. È importante fare attenzione all'utilizzo delle porte sulla macchina, poiché non è possibile permettere a due o più applicazioni di condividere la stessa coppia indirizzo/porta di ascolto. In particolare i moduli possono presentare dei malfunzionamenti qualora la coppia indirizzo/porta specificata come server sia già in uso da qualche altro processo. Se questo accade occorre cambiare i parametri associati al modulo, oppure le impostazioni dell'altro processo. Tipicamente il problema si risolve cambiando uno dei parametri in questione e riconfigurando i client che utilizzano quel servizio in modo da aggiornarli al cambiamento. Se è necessario cambiare un indirizzo IP ma la macchina ha una sola scheda di rete con un solo indirizzo IP associato, bisognerà aggiungere altri indirizzi alla scheda (e quindi alla macchina) attraverso le impostazioni di rete di Windows (sezione avanzate).

Il menu server presenta le seguenti azioni:

- Modifica: Permette di alterare una voce già inserita nella lista.
- Inserisci: Permette di aggiungere una voce alla lista dei server. Ogni voce consiste in un indirizzo IP di ascolto e di una porta.
- Rimuovi: Permette di eliminare una voce dalla lista.
- Rimuovi tutto: Permette di eliminare tutte le voci dalla lista.

Regole di accesso

La regole di accesso, note anche come ACL (Access Control List), vengono impiegate per stabilire i permessi sugli utenti/macchine che utilizzano il servizio. In particolare è possibile stabilire, per quel che riguarda il modulo WEB, chi può navigare, quali siti può visitare e in quale fascia oraria della giornata.

Le regole di accesso sono liste di voci ognuna delle quali è una coppia (condizione, azione). Quando la condizione viene verificata (match) l'azione associata viene eseguita. Esempi di condizioni possono essere: uno o più indirizzi IP di client che si collegano, siti a cui gli utenti si vogliono collegare definiti attraverso un qualche criterio, un particolare intervallo temporale nell'arco della giornata o anche combinazioni più complesse.

Le azioni associate invece possono essere solo "Permetti" o "Blocca". Quando un particolare client si collega al modulo per richiedere un servizio, la lista delle voci viene scorsa dalla prima in avanti e se una di esse ha una condizione che risulta verificata l'azione associata viene eseguita. Il risultato ottenuto è quello di avere la richiesta del client accettata (e quindi il modulo procede a fornire quanto richiesto) oppure rifiutata: in tal caso il client ottiene come risposta un messaggio di errore che lo informa che la richiesta non può essere soddisfatta.

L'ordine con cui vengono inserite le voci è importante poiché la prima condizione verificata è quella che stabilisce se la richiesta del client può essere o meno soddisfatta.

Se nessuna delle voci della lista è applicabile esiste un'ultima voce implicita la cui condizione assorbe tutto, che ha come regola associata un "Blocca". In altre parole, se non vi è nessun match nelle condizioni definite dall'utente, la risposta è un rifiuto. Se si desidera invertire il comportamento ed avere un default "Permetti", cioè accettare tutto ciò che non viene esplicitamente vietato, è sufficiente inserire una voce in ultima posizione la cui condizione assorbe tutto e la cui azione associata è un "Permetti".

Se si desidera passare ad esempi pratici di impiego delle regole si puo vedere la sezione chiamata «Regole di accesso per il WEB».

Inizialmente la tabella contiene una sola voce che permette tutto. Selezionando tale voce, cliccando sopra la linea, si evidenzierà (sfondo giallo) e a quel punto sarà possibile modificarne i valori (tasto Modifica sul bordo superiore) oppure impartire altri comandi. È possibile duplicare una riga usando Duplica e poi modificare la nuova voce per creare una regola basata su una presesistente.

Le voci sul bordo superiore "Inserisci sopra", "Inserisci sotto", "Sposta sopra" e "Sposta sotto" vengono utilizzate per inserire o cambiare l'ordine delle voci nella tabella.

Affinchè i cambiamenti vengano posti in essere, è necessario riavviare il modulo (in quanto solo all'avvio i file di configurazione vengono letti).

Attraverso la voce Modifica o Inserisci sopra/Inserisci sotto è possibile accedere al pannello di editing delle voci della tabella.

Il pannello per l'editing della voce si divide in 6 sezioni. Le sezioni "Sorgente", "Destinazione", "Intervalli temporali" e "Utenti" definiscono la condizione relativa a quella particolare voce della tabella. La voce "Azione", come dice il nome stesso, definisce invece l'azione associata. Utilizzare la voce "Commento" per inserire una nota esplicativa della regola.

- Abilitazione o disabilitazione di una regola. È possibile abilitare o disabilitare una regola senza rimuoverla dall'elenco. Una regola abilitata è contrassegnata da una spunta verde mentre una disabilitata è indicata da una croce rossa. Cliccando sul simbolo è possibile cambiarne lo stato.

  Sorgente: Definisce l'insieme dei client che possono connettersi al modulo. È possibile definire l'insieme dei client attraverso il loro indirizzo IP, definendoli singolarmente come un insieme di 4 interi fra 0 e 255, oppure mediante una subnet cioè un insieme di indirizzi IP. La subnet si può definire mediante l'uso del carattere '*' che indica un valore qualunque compreso tra 0 e 255 in numero tale da formare un indirizzo IP valido: ad esempio 10.1.* indica un qualunque indirizzo IP avente come primi due numeri 10 e 1. Un insieme di indirizzi IP può essere rappresentato anche come

intervallo, quindi è possibile scrivere 10.1.1.3−8 indicando così gli indirizzi 10.1.1.3, 10.1.1.4, 10.1.1.5, 10.1.1.6, 10.1.1.7 e 10.1.1.8. Oppure è possibile adottare la notazione NSC; ad esempio per indicare tutti gli indirizzi aventi come primi due numeri 10 e 1 si scriverà 10.1.0.0/16, dove il numero successivo al carattere "/" indica il numero di bit a 1 della subnet mask a partire da quello più significativo. Quindi se la subnet mask fosse 255.0.0.0 sarà 8; con 255.255.0.0 sarà 16; con 255.255.255.0 sarà 24 e con 255.255.255.255 sarà 32 (quindi l'indirizzo esatto che precede il carattere di "/"). Siccome ogni host oltre all'indirizzo IP può avere associato un nome, è possibile creare regole basaste su questo. Utilizzando una simple expression o una più complessa regular expression è possibile riconoscere nomi aventi determinate caratteristiche (ad esempio *.example.com identifica un qualunque nome nel dominio example.com). Per avere maggiori informazioni riguardo simple expression e regular expression vedere Capitolo 9, *Pattern matching*. Se non si desidera imporre vincoli sulla sorgente, lasciare indicato "Tutti" nel box a fianco. Oltre all'host è possibile anche definire una porta, che sarà la porta utilizzata dal client per connettersi (solitamente i client utilizzano delle porte sorgenti sempre diverse, per questo motivo questa impostazione viene raramente utilizzata).

- Destinazione: Analogamente alla sorgente, la destinazione consente di imporre vincoli sui server che il client può contattare attraverso il modulo utilizzando un'analoga struttura.

  Inoltre per il modulo WEB è disponibile una ulteriore voce (Categorizzazione) che consente di imporre vincoli anche sulla natura del sito che viene contattato e non solo quindi in base al nome o all'indirizzo IP.

  Se si desiderano ulteriori informazioni sul categorizzatore e in particolare su come utilizzare le categorie definibili dall'utente (*Userdef01, ..., Userdef10* sotto Sistema/Categorizzatore Web) vedere la sezione chiamata «DB Utente».
- Azione: L'azione definisce cosa fare nel caso le condizioni vengano tutte quante verificate. Le scelte sono due: "Blocca" o "Permetti".
- Intervalli temporali: Permette di definire una fascia oraria in cui la condizione sarà valida. Il pannello sulla destra indica quale tipo di intervallo inserire e il pannello sulla sinistra indica la lista degli intervalli considerati dalla regola.
- Utente: È possibile richiedere l'autenticazione utente. È possibile eseguire l'autenticazione usando il database utenti di un WorkGroup, di un Dominio NT o di un dominio Active Directory (Windows 2000/2003). Se si seleziona di utilizzare un dominio o workgroup, verranno visualizzati tutti i domini e workgroup raggiungibili. Con un doppio click sarà possibile selezionare l'utente o il gruppo desiderato da inserire nella regola. Può capitare che ad un certo punto eXtensiveControl® necessiti delle credenziali di un utente autorizzato a sfogliare le risorse del domain controller. Quando questo accade verrà visualizzato un box ove sono richiesti questi dati. Scegliendo invece come tipo di autenticazione il valore "Locale", è possibile utilizzare un'autenticazione per l'appunto locale, quindi specificata all'interno del prodotto. Nella sezione "Sistema" è presente una sotto−sezione "Utenti locali" dove è possibile specificare localmente all'interno di eXtensiveControl® gli utenti e i gruppi da utilizzare all'interno del software. A differenza dell'autenticazione tramite dominio o workgroup in questo caso è possibile inserire solamente gruppi.
- Commento: In questo spazio l'utente può inserire un commento.

Quando si termina l'editing della voce è possibile confermare il tutto con il tasto "Conferma" sul bordo inferiore del pannello, oppure annullare l'inserimento/modifica con "Annulla".

Visualizzatore Log

La sezione Visualizzatore Log è divisa in 3 sotto sezioni che hanno funzionamento analogo fra loro, cioè quella di permettere la visualizzazione dei dati registrati nei 3 diversi file di log generati.

- Log: mostra il contenuto del file di log dove vengono registrate le attività dei proxy, in particolare essi tengono traccia delle azioni svolte dai client. Il formato segue lo standard Welf, pertanto suddetti file

possono essere utilizzati per compilare report non solo dal motore interno di eXtensiveControl® ma anche da programmi di terze parti che supportano il formato Welf.
- Comandi: questa sezione mostra il contenuto del file comandi; nel file comandi vengono registrate informazioni aggiuntive rispetto al file di log, che per motivi di compatibilità col formato Welf non possono essere inserite direttamente nel file di log.
- Debug: mostra il contenuto del file di debug. Questo file risulta particolarmente indicato per diagnosticare eventuali problemi di funzionamento del modulo. La quantità di informazioni registrate nel file dipende dal livello di debug impostato nel menu Avanzate. Più il livello di debug è alto, maggiori saranno le informazioni registrate nel file (ma anche lo spazio occupato su disco, mentre le prestazioni del sistema tendono invece a calare). Solitamente si alza il livello di debug quando si presentano problemi di funzionamento e il numero di informazioni con il livello di default risulta essere insufficiente.

Tutti e tre i pannelli presentano la medesima interfaccia che si compone di tre voci:

- Punto di inizio della lettura: Permette di stabilire da quale punto del file iniziare la visualizzazione. È possibile visualizzare il contenuto dall'inizio del file, dalla fine o a partire da una linea specificata dall'utente.
- Numeri di linee: Numero di linee che l'utente intende visualizzare. Ad esempio impostando tale valore a 10 e la visualizzazione a partire dalla fine del file, si otterranno le ultime 10 linee del file. Tipicamente questa è la scelta più comune in quanto spesso si vogliono visualizzare le linee in prossimità di un errore appena avvenuto e che si trova dunque alla fine del file.
- Risoluzione dei nomi: Con questa impostazione gli indirizzi IP vengono risolti in hostname in modo da essere più esplicativi. Ad esempio l'amministratore potrebbe voler sapere su quali siti navigano i suoi utenti (e non accontentarsi degli indirizzi IP). Non sempre è possibile risalire al nome di un host conoscendone l'indirizzo IP.

Capitolo 7. Funzionamento del modulo POP3

Introduzione

Il modulo POP3 viene tipicamente impiegato per filtrare la posta dei client durante il download dei messaggi (che tipicamente avviene da un server esterno). La principale differenza fra il modulo SMTP ed il modulo POP3 consiste nel fatto che nel primo caso chi si collega al modulo STMP (i client sia interni che esterni) lo fa per spedire posta, nel secondo caso invece chi si collega al modulo POP3 lo fa per ricevere posta.

Il modulo POP3 viene tipicamente utilizzato con server di posta esterni, in quanto la posta non può essere controllata prima che arrivi sul server stesso ed il POP3 risulta quindi l'unica opzione per effettuare il controllo sui messaggi in ingresso. Nel caso di un server interno invece è possibile imporre dei controlli sia sul protocollo POP3 che sul protocollo SMTP tuttavia quest'ultimo è preferibile dal momento che permette di applicare le policy aziendali prima che i mesaggi arrivino sul server interno.

Configurazione del modulo POP3

Esistono due tipi di configurazione per il modulo POP3, a seconda che gli utenti necessitino di scaricare la posta da un solo server o da più server distinti.

- *In caso di un singolo server* è sufficiente che il client sia configurato per utilizzare il modulo POP3 come server in ingresso (inbound mail) e il modulo deve essere configurato per utilizzare come Server di default (vedere anche la sezione chiamata «Server») il server esterno su cui la posta è depositata.
- *In caso di server multipli* in questo caso il client dovrà sempre essere configurato per utilizzare il modulo POP3 come server in ingresso (inbound mail), tuttavia occorre anche:

- lasciare vuoto il box Server di default della sezione Server, vedere anche la sezione chiamata «Server»)
- cambiare nelle impostazioni del client lo username relativo ad ogni account aggiungendo il suffisso */<serverpop3>*, facendo attenzione che il carattere */* può cambiare a seconda di quello che è definito alla voce Separatore account/server nella sezione Avanzate del POP3 (vedere la sezione chiamata «Avanzate»), mentre <serverpop3> indica il nome o l'indirizzo IP del server POP3 che l'utente desidera contattare per ricevere la posta.

Si supponga ad esempio che l'utente *user01* desideri prelevare la posta dal server POP3 esterno *server01.com* mentre l'utente *user02* desidera prelevare la posta dal server *server02.com*. Per far questo, dopo essersi accertati che non vi sia alcun "server di default" configurato nella sezione Server del modulo POP3, occorrerà cambiare il nome dell'account utente sui rispettivi client di posta in modo che sia: *user01/server01.com* e *user02/server02.com*.

Se un utente dovesse avere uno username che contiene al suo interno il carattere "/", sarà necessario cambiare il carattere di separazione nella sezione Avanzate del Modulo POP3 e modificare di conseguenza il nome dell'account sul client di posta.

Se si desidera conoscere i dettagli su come configurare il modulo e/o il significato dei vari parametri, vedere Capitolo 8, *Modulo POP3*

Capitolo 8. Modulo POP3

Il modulo POP3 viene utilizzato per filtrare le mail che i client di posta scaricano da uno o più server POP3. In questa sezione verranno forniti i dettagli sul significato dei vari parametri di configurazione. Se si desidera un'introduzione generica al modulo POP3 vedere Capitolo 7, *Funzionamento del modulo POP3*.

Info

La sezione Info presenta un riepilogo dello stato del modulo:

- Stato: Lo stato del modulo può essere: Disabilitato, Fermo, Avviato o In avvio.
- Data di avvio: L'ultima volta che il modulo è stato avviato.
- Dimensioni file di log: Spazio occupato su disco dal file .log.
- Dimensioni file comandi processati: Spazio occupato su disco dal file comandi (estensione .lcd).
- Dimensioni file di debug: Spazio occupato su disco dal file con le informazioni di debug (estensione .err).

Ogni modulo, quando avviato, registra le informazioni relative al proprio funzionamento su tre file che portano il nome del modulo stesso ed estensioni (.log, .lcd e .err) dipendenti dal tipo di dati che raccolgono. Ogni giorno, ad un orario stabilito (che può essere variato a piacere) i file vengono rinominati e viene aggiunta la data corrente nel nome del file e poi viene creato un nuovo file senza data per il nuovo giorno. In questo modo i file si accumulano giorno per giorno e possono essere facilmente identificati dalla data che hanno nel nome stesso. Per default la rotazione avviene alle 23.58, quindi il file rinominato avrà la data corrente e tutte le informazioni relative a quel giorno (almeno fino alle 23:58) e gli ultimi 2 minuti del giorno precedente. In questo modo si otterranno dei file con riportata nel nome una data e all'interno di essi tutti i log relativi alla data indicata nel nome.

Nella parte inferiore della sezione è possibile accedere alle statistiche del modulo nell'ultima ora, giorno e settimana. Viene fornito un riassunto grafico delle attività del modulo, in modo da riconoscere immediatamente eventuali picchi di traffico, oltre al valore minimo, massimo e medio dell'attività visualizzata. "Tipo" specifica la caratteristica del modulo che si vuole visualizzare e "Intervallo" l'intervallo temporale che si desidera considerare nella statistica. "Visualizza statistiche" mostra le statistiche desiderate.

Avanzate

Significato dei parametri disponibili:

- Durata massima di una connessione: durata massima in secondi di una connessione. Un valore pari a 0 indica un tempo infinito
- Durata massima di una connessione inattiva: tempo massimo in secondi dopo il quale una connessione viene terminata se non vengono ricevuti dei dati.
- Livello di debug: regola la quantità di log che viene generata dal modulo (file .err). Più piccolo è tale valore, minori sono le informazioni registrate. Tipicamente si aumenta il livello di debug in fase di diagnostica per capire la causa di un problema.
- Consenti host per cui non esiste il nome: può capitare che eXtensiveControl® debba eseguire una query DNS inversa da indirizzo IP a nome per applicare la politica di accesso definita nella sezione Regole di accesso. Questo accade ad esempio se si imposta una politica basata sui nomi delle macchine piuttosto che sui loro indirizzi IP. Se la conversione fallisce la connessione viene rifiutata a meno che questo flag non venga impostato.
- Separatore account/server: carattere utilizzato per separare username e server POP3, è usato quando l'utente vuole connettersi a più server POP. Vedere anche la sezione chiamata «Server» e la sezione chiamata «Configurazione del modulo POP3»
- Abilita comando TOP: il comando TOP viene utilizzato quando il client di posta desidera scaricare solo parte del messaggio (ad esempio per prendere visione dell'intestazione ed eventualmente evitare di scaricare messaggi di grandi dimensioni se si ha il sospetto che sia posta indesiderata).

Dopo avere cambiato la configurazione per salvare le modifiche è necessario premere il pulsante Salva. Il pulsante "Annulla le modifiche" effettua una rilettura della configurazione presente su disco cancellando così le modifiche inserite e non ancora salvate.

Server

I server vengono utilizzati per associare ad un dato modulo uno o più indirizzi e porte di ascolto. Quando un client deve utilizzare un modulo per accedere ad un dato servizio deve infatti conoscere l'indirizzo e la porta TCP a cui connettersi per inviare le richieste. Tali parametri vengono configurati in questa sezione e sono specifici per ogni modulo. È importante fare attenzione all'utilizzo delle porte sulla macchina, poiché non è possibile permettere a due o più applicazioni di condividere la stessa coppia indirizzo/porta di ascolto. In particolare i moduli possono presentare dei malfunzionamenti qualora la coppia indirizzo/porta specificata come server sia già in uso da qualche altro processo. Se questo accade occorre cambiare i parametri associati al modulo, oppure le impostazioni dell'altro processo. Tipicamente il problema si risolve cambiando uno dei parametri in questione e riconfigurando i client che utilizzano quel servizio in modo da aggiornarli al cambiamento. Se è necessario cambiare un indirizzo IP ma la macchina ha una sola scheda di rete con un solo indirizzo IP associato, bisognerà aggiungere altri indirizzi alla scheda (e quindi alla macchina) attraverso le impostazioni di rete di Windows (sezione avanzate).

Nel modulo POP3 è possibile definire anche un server di default per ogni server. Il server di default viene utilizzato quando si desidera impostare un unico server di riferimento che gli utenti possono utilizzare per prelevare la posta. Nel caso invece si voglia utilizzare più di un server, allora è necessario lasciare vuoto tale campo e impostare nella sezione Avanzate il Separatore account/server (se non si vuole utilizzare il valore di default "/"). In quest'ultimo caso l'utente può infatti indicare l'host al quale vuole effettuare la connessione utilizzando come username la forma *account/server* (il carattere "/" deve essere sostituito dal carattere configurato in Separatore account/server), dove account indica il nome utente e server l'indirizzo o il nome del computer sul quale è installato il server POP3.

Il menu Server presenta le seguenti azioni:

- Modifica: Permette di alterare una voce già inserita nella lista.
- Inserisci: Permette di aggiungere una voce alla lista dei server. Ogni voce consiste in un indirizzo IP di ascolto e di una porta.
- Rimuovi: Permette di eliminare una voce dalla lista.
- Rimuovi tutto: Permette di eliminare tutte le voci dalla lista.

Regole di accesso

Le regole di accesso, note anche come ACL (Access Control List), vengono impiegate per impostare le policy di utilizzo del protocollo POP3. In particolare è possibile stabilire, per quel che riguarda il modulo POP3, chi può scaricare la posta elettronica, da quale server e in quale fascia del giorno.

Alla base del funzionamento delle ACL ci sono alcune regole che devono essere assimilate per poter configurare correttamente il modulo: in particolare è di fondamentale importanza capire le precedenze con cui queste regole vengono applicate.

Le ACL sono liste di voci ognuna delle quali è una coppia (condizione, azione). Quando la condizione viene verificata (match) l'azione associata viene eseguita. Esempi di condizioni possono essere: uno o più indirizzi IP di client che si possono collegare, server che gli utenti possono raggiungere, un particolare intervallo temporale nell'arco della giornata o anche combinazioni più complesse.

Le azioni associate invece possono essere solo "Permetti" o "Blocca". Quando un particolare client si collega al modulo per richiedere un servizio, la lista delle voci viene scorsa dalla prima in avanti e se una di esse ha una condizione che risulta verificata l'azione associata viene eseguita. Il risultato ottenuto è quello di avere la richiesta del client accettata (e quindi il modulo procede a fornire quanto richiesto) oppure rifiutata: in tal caso il client ottiene come risposta un messaggio di errore che lo informa che la richiesta non può essere soddisfatta.

L'ordine con cui vengono inserite le voci è importante poiché la prima condizione verificata è quella che stabilisce se la richiesta del client può essere o meno soddisfatta.

Se nessuna delle voci della lista è applicabile esiste un'ultima voce implicita la cui condizione assorbe tutto, che ha come regola associata un "Blocca". In altre parole, se non vi è nessun match nelle condizioni definite dall'utente, la risposta è un rifiuto. Se si desidera invertire il comportamento ed avere un default "Permetti", cioè accettare tutto ciò che non viene esplicitamente vietato, è sufficiente inserire una voce in ultima posizione la cui condizione assorbe tutto e la cui azione associata è un "Permetti".

Le condizioni che possono essere espresse all'interno della lista dipendono da quale modulo esse sono associate. Ad esempio nel caso del filtro web sarà possibile esprimere come condizioni oltre agli indirizzi IP del sorgente e del destinatario anche (ad esempio) la tipologia del sito di destinazione. Questa opzione non è invece disponibile per il modulo POP3, perché in tale contesto priva di significato.

Selezionando "Regole di accesso" è possibile vedere la tabella con le voci che compongono la policy di accesso. Inizialmente tale tabella contiene una sola voce che permette tutto a tutti. Selezionando tale voce, la linea verrà evidenziata (sfondo giallo) e a questo punto sarà possibile modificarne i valori (tasto Modifica sul bordo superiore) oppure rimuoverla.

Affinchè i cambiamenti vengano recepiti deve essere riavviato il modulo (in quanto solo all'avvio i file di configurazione vengono letti).

Le voci sul bordo superiore "Inserisci sopra", "Inserisci sotto", "Sposta sopra" e "Sposta sotto" vengono utilizzate per inserire o cambiare l'ordine delle voci nella tabella.

Attraverso la voce "Modifica" o "Inserisci sopra"/"Inserisci sotto" è possibile accedere al pannello di editing delle voci della tabella.

Il pannello per l'editing della voce si divide in 5 sezioni: "Sorgente", "Destinazione" e "Intervalli temporali" per definire la condizione relativa a quella particolare voce della tabella, "Azione" definisce l'azione associata e "Commento" per inserire una nota esplicativa della regola.

- Abilitazione o disabilitazione di una regola. È possibile abilitare o disabilitare una regola senza rimuoverla dall'elenco. Una regola abilitata è contrassegnata da una spunta verde mentre una disabilitata è indicata da una croce rossa. Cliccando sul simbolo è possibile cambiarne lo stato.

  Sorgente: Definisce l'insieme dei client che possono connettersi al modulo. È possibile definire l'insieme dei client attraverso il loro indirizzo IP, definendoli singolarmente come un insieme di 4 interi fra 0 e 255, oppure mediante una subnet cioè un insieme di indirizzi IP. La subnet si può definire mediante l'uso del carattere '*' che indica un valore qualunque compreso tra 0 e 255 in numero tale da formare un indirizzo IP valido: ad esempio 10.1.* indica un qualunque indirizzo IP avente come primi due numeri 10 e 1. Un insieme di indirizzi IP può essere rappresentato anche come intervallo, quindi è possibile scrivere 10.1.1.3–8 indicando così gli indirizzi 10.1.1.3, 10.1.1.4, 10.1.1.5, 10.1.1.6, 10.1.1.7 e 10.1.1.8. Oppure è possibile adottare la notazione NSC; ad esempio per indicare tutti gli indirizzi aventi come primi due numeri 10 e 1 si scriverà 10.1.0.0/16, dove il numero successivo al carattere "/" indica il numero di bit a 1 della subnet mask a partire da quello più significativo. Quindi se la subnet mask fosse 255.0.0.0 sarà 8; con 255.255.0.0 sarà 16; con 255.255.255.0 sarà 24 e con 255.255.255.255 sarà 32 (quindi l'indirizzo esatto che precede il carattere di "/"). Siccome ogni host oltre all'indirizzo IP può avere associato un nome, è possibile creare regole basate su questo. Utilizzando una simple expression o una più complessa regular expression è possibile riconoscere nomi aventi determinate caratteristiche (ad esempio *.example.com identifica un qualunque nome nel dominio example.com). Per avere maggiori informazioni riguardo simple expression e regular expression vedere Capitolo 9, *Pattern matching*. Se non si desidera imporre vincoli sulla sorgente, lasciare indicato "Tutti" nel box a fianco. Oltre all'host è possibile anche definire una porta, che sarà la porta utilizzata dal client per connettersi (solitamente i client utilizzano delle porte sorgenti sempre diverse, per questo motivo questa impostazione viene raramente utilizzata).
- Destinazione: Analogamente alla sorgente; la destinazione consente di imporre vincoli sui server che il client può contattare attraverso il modulo mediante gli stessi formalismi.
- Azione: L'azione definisce cosa fare nel caso la condizione venga soddisfatta. Le scelte sono due: "Blocca" o "Permetti".
- Intervalli temporali: Permette di definire una fascia oraria in cui la condizione è valida. Il box sulla destra indica quale tipo di intervallo inserire e il box sulla sinistra indica la lista degli intervalli considerati.
- Commento: In questo spazio l'utente può inserire un commento allo scopo di chiarire (ad esempio) il perché di una data voce.

Quando si termina l'editing della voce è possibile confermare il tutto con il tasto "Conferma" sul bordo inferiore del pannello, oppure annullare l'inserimento/modifica con il tasto "Annulla".

Filtro email

In questa sezione sono presenti tre sottosezioni principali. La sezione Avanzate parametrizza il comportamento dei filtri definendone dei parametri generici mentre le altre due definiscono i filtri applicati agli header e agli allegati. Ogni volta che arriva un messaggio viene prima applicato il filtro sugli header e poi quello sugli allegati.

Avanzate

La sezione Avanzate permette di definire dei parametri che modificano il comportamento dei filtri sugli header e sugli allegati. I parametri sono:

- Disabilita controllo sul path assoluto: talvolta capita che nel messaggio il nome dell'allegato contenga riferimenti (path) assoluti. Se questa voce viene abilitata, il messaggio viene lasciato passare anche se questo accade, altrimenti viene bloccato dal filtro sugli allegati senza che le regole di quest'ultimo vengano applicate. In altre parole il controllo sul path assoluto ha la precedenza sulle regole associate al filtro.
- Disabilita controllo sui nomi in Content−Type: esistono due campi per specificare il nome di un allegato nel formato MIME; se i due campi in questione sono in disaccordo, il messaggio viene lasciato passare solo se il box in questione è spuntato, altrimenti viene bloccato dal filtro sugli allegati prima di applicarne le regole.
- Numero massimo di estrazioni ricorsive negli archivi: indica fino a che livello di ricorsività estrarre gli archivi (ad esempio .zip) che contengono altri archivi, che contengono altri achivi, etc...
- Filtra anche il contenuto degli archivi: applica le stesse regole degli allegati anche al contenuto degli archivi. Per esempio, se si vietano le estensioni .doc, e se questa casella non è spuntata, un .doc all'interno di un file .zip non viene rilevato. Se tale opzione invece è attiva, allora il file viene riconosciuto.
- Blocca file crittati: Quarantena tutti gli allegati crittati, anche se contenuti in un archivio.

Filtro sugli Header

Il filtro sugli header permette di eseguire determinate azioni in base al contenuto di header indicati.

Col pulsante Aggiungi è possibile inserire un numero a piacere di condizioni che dovranno essere tutte quante verificate affinché l'azione associata venga eseguita. Tali condizioni riguardano gli header del messaggio e sono:

- To o Cc: viene verificato il campo "To"("A") e "CC" ("CopiaConoscenza") del messaggio.
- Cc: campo "CopiaConoscenza" del messaggio.
- Subject: campo "Oggetto" del messaggio.
- Body: corpo del messaggio, si intende tutto ciò che non comprende gli header.
- From: è il mittente dichiarato (non necessariamente quello reale) del messaggio.
- To: campo "To" del messaggio.
- Categoria link: verifica la presenza di link all'interno del messaggio relativi a siti di determinate categorie.
- Libero: se si seleziona il suddetto campo sarà possibile digitare nel box che compare a fianco il testo che identifica il nome dell'header (può tornare utile quando si vogliono utilizzare header non supportati nativamente dal prodotto).

Ogni sottosezione accetta tre tipi diversi di input, vale a dire delle *simple expression*, delle *regular expression* e delle *case sensitive simple expression*. Se si desiderano informazioni sulla sintassi di questi costrutti, oppure avere una panoramica generale delle stesse vedere Capitolo 9, *Pattern matching*

Le possibili azioni associate a questo filtro sono:

- Continua: vengono saltate le rimanenti regole e si passa al filtro successivo (che in questo caso è il filtro AntiVirus).
- Elimina: il messaggio viene eliminato.
- Permetti: il messaggio viene accettato e quindi viene inviato all'utente che sta scaricando la posta.
- Quarantena: il messaggio viene trasferito nella sezione quarantena "email bloccate" e dovrà essere gestito dall'amministratore, che deciderà se rilasciarlo o eliminarlo.

Filtro sugli Allegati

Permette di filtrare i messaggi in base al contenuto degli allegati. Una volta selezionata una regola si passa a un pannello nel quale è possibile impostare oltre al "From" e al "To" una serie di condizioni ulteriori sul tipo di allegato. Da notare che in questo caso, a differenza del modulo SMTP, il "From" e il "To" si riferiscono ai dati dichiarati negli header. I pulsanti Aggiungi e Rimuovi permettono l'inserimento di condizioni aggiuntive alle regole presenti. Ogni condizione può essere del tipo:

- From: la condizione è applicata al campo "From" dell'header del messaggio.
- To: la condizione è applicata al campo "To" dell'header del messaggio.
- Nome dell'allegato: la condizione è applicata al nome del file allegato.
- Dimensione del messaggio: la condizione è applicata alla dimensione dell'intero messaggio, imponendo un vincolo sulla sua dimensione e richiedendo che sia più grande o più piccolo di un determinato valore.
- Tipo dell'allegato: la condizione è applicata al tipo di file (apparirà a fianco una lista di tipi di file conosciuti). È importante ricordare che la tipologia viene dedotta dalla struttura interna del file e non dalla sua estensione.

Il filtro sugli allegati permette di effettuare le stesse azioni del filtro precedente (quello sugli header) e accetta la stessa forma di regular expression per la definizione delle regole.

Se nessuna delle condizioni in questa sottosezione viene verificata, il programma passa all'elaborazione del messaggio con il filtro successivo (in questo caso l'AntiVirus).

AntiVirus

Il filtro AntiVirus permette di bloccare le mail contenenti virus, worm o altro codice dannoso.

La sezione si compone di due sottosezioni: Generale ed Eccezioni. La sottosezione Generale è composta delle seguenti voci:

- Controllo AntiVirus: spuntare questa casella per abilitare il controllo AntiVirus. Se manca la spunta le rimanenti opzioni perdono di significato e vengono pertanto ignorate.
- Tempo massimo di scansione (sec.): se l'antivirus non restituisce una risposta entro il tempo specificato in questa casella, la mail viene considerata infetta.
- Comando AntiVirus (con path): in questo box occorre digitare il nome dell'eseguibile che da linea di comando deve essere lanciato per effettuare la scansione antivirus.
- Parametri del comando AntiVirus : in questo box è possibile digitare i parametri che si desiderano passare al motore antivirus quando viene avviata la scansione di un allegato.

La sottosezione Eccezioni permette di specificare uno o più indirizzi e−mail o domini che saranno esclusi dal controllo antivirus (quando presenti come destinazione). Se si specifica un dominio tutti gli indirizzi destinati al dominio o ad uno dei sottodomini verranno esclusi dal controllo (es: indicando example.com gli indirizzi user01@example.com e user02@under.example.com non saranno controllati).

Se eXtensiveControl® rileva la presenza di un AntiVirus supportato riempie automaticamente i campi Comando AntiVirus e Parametri del comando AntiVirus.

Se né il messaggio né gli allegati contenuti risultano infetti, l'analisi prosegue con il filtro antispam.

AntiSpam

La sezione si divide nelle seguenti sottosezioni:

- Generale: Questa sottosezione si compone dei seguenti parametri:
    - Controllo AntiSpam: questa casella determina se il filtro antispam è attivo. Se questa casella non fosse spuntata il resto delle impostazioni perderebbe di significato.
    - Marcatore dello Spam inserito nel subject: Indica la stringa che viene inserita come prefisso nel subject dei messaggi riconosciuti come spam. Per default tale valore è "[SPAM]".
    - Soglia di Spam: Indica la soglia oltre la quale il messaggio è considerato spam.
- Whitelist: si tratta di una lista di domini o indirizzi di posta dai quale i messaggi vengono automaticamente riconosciuti come buoni con un peso di spam pari a 0 (il valore minimo).
- Backlist: si tratta di una lista di domini o indirizzi di posta dai quale i messaggi vengono automaticamente riconosciuti come spam con un peso di spam pari a 100 (il valore massimo).
- Aggiornamento DB: questa sezione è un collegamento alla sezione Symbolic DB all'interno della voce AntiSpam della sezione Sistema e permette di effettuare un aggiornamento del database di spam, di pianificare il download in automatico e di configurare l'uso di un server proxy se è necessario per comunicare con Internet.

Il tasto Annulla le modifiche legge la configurazione correntemente presente sul disco cancellando le modifiche inserite fino a quel momento e non ancora salvate, mentre il tasto Salva scrive la configurazione impostata nel file di configurazione.

AntiPhishing

Questa sezione abilita il fitraggio antiphishing sulla posta scaricata ed è composta dalle seguenti sezioni:

- Generale:
    - Controllo AntiPhishing: questo checkbox abilita il controllo AntiPhishing sul traffico POP3.
    - Marcatore del Phishing inserito nel subject: questo form permette di specificare il tag da inserire nel subject delle mail ritenute phishing.
- Aggiornamento DB: questa sezione è un collegamento alla sezione Symbolic DB all'interno della voce AntiPhishing della sezione Sistema e permette di effettuare un aggiornamento del database, di pianificare il download in automatico e di configurare l'uso di un server proxy se è necessario per comunicare con Internet.

Il tasto Annulla le modifiche legge la configurazione correntemente presente sul disco cancellando le modifiche inserite e non ancora salvate, mentre il tasto Salva scrive la configurazione impostata nel file di configurazione.

Quarantena

La sezione di quarantena permette di gestire i messaggi che vengono bloccati e quarantenati da uno dei filtri applicati alla posta.

In questa sezione è possibile effettuare le seguenti azioni:

- Rimuovi tutto: elimina tutti i messaggi che sono stati messi in quarantena.
- Rimuovi tutti i messaggi infetti: cancella tutti i messaggi sicuramente infetti. I messaggi posti in quarantena dai filtri o per i quali il controllo antivirus non ha fornito il responso di sicuremente infetti non sono cancellati.

Sono presenti le seguenti sezioni:

- Email bloccate: questa sezione mostra i messaggi che vengono messi in quarantena perché ritenuti

infetti o perché bloccati dalle regole di filtraggio sugli header o sugli allegati. Le tre righe presenti permettono di cercare per: id del messaggio, coda di messaggi più recenti (mostra gli ultimi n messaggi, dove n viene inserito nel box a fianco), oppure mostra i messaggi ricevuti nelle ultime m ore.

Visualizzatore Log

La sezione Visualizzatore Log è divisa in 3 sotto sezioni che hanno funzionamento analogo fra loro, cioè quella di permettere la visualizzazione dei dati registrati nei 3 diversi file di log generati.

- Log: mostra il contenuto del file di log dove vengono registrate le attività dei proxy, in particolare essi tengono traccia delle azioni svolte dai client. Il formato segue lo standard Welf, pertanto suddetti file possono essere utilizzati per compilare report non solo dal motore interno di eXtensiveControl® ma anche da programmi di terze parti che supportano il formato Welf.
- Comandi: questa sezione mostra il contenuto del file comandi; nel file comandi vengono registrate informazioni aggiuntive rispetto al file di log, che per motivi di compatibilità col formato Welf non possono essere inserite direttamente nel file di log.
- Debug: mostra il contenuto del file di debug. Questo file risulta particolarmente indicato per diagnosticare eventuali problemi di funzionamento del modulo. La quantità di informazioni registrate nel file dipende dal livello di debug impostato nel menu Avanzate. Più il livello di debug è alto, maggiori saranno le informazioni registrate nel file (ma anche lo spazio occupato su disco, mentre le prestazioni del sistema tendono invece a calare). Solitamente si alza il livello di debug quando si presentano problemi di funzionamento e il numero di informazioni con il livello di default risulta essere insufficiente.

Tutti e tre i pannelli presentano la medesima interfaccia che si compone di tre voci:

- Punto di inizio della lettura: Permette di stabilire da quale punto del file iniziare la visualizzazione. È possibile visualizzare il contenuto dall'inizio del file, dalla fine o a partire da una linea specificata dall'utente.
- Numeri di linee: Numero di linee che l'utente intende visualizzare. Ad esempio impostando tale valore a 10 e la visualizzazione a partire dalla fine del file, si otterranno le ultime 10 linee del file. Tipicamente questa è la scelta più comune in quanto spesso si vogliono visualizzare le linee in prossimità di un errore appena avvenuto e che si trova dunque nelle alla fine del file.
- Risoluzione dei nomi: Con questa impostazione gli indirizzi IP vengono risolti in hostname in modo da essere più esplicativi. Ad esempio l'amministratore potrebbe voler sapere su quali siti navigano i suoi utenti (e non accontentarsi degli indirizzi IP). Non sempre è possibile risalire al nome di un host conoscendone l'indirizzo IP.

Capitolo 9. Pattern matching

Introduzione

Questa sezione tratta la sintassi con cui è possibile esprimere una condizione da verificare (pattern matching), in particolare vengono prese in considerazione le *simple expression*, le *regular expression* e le *case sensitive simple expression*

L'idea alla base del *pattern matching* è quella di utilizzare regole che consentano di esprimere condizioni sulle stringhe in modo semplice e flessibile. Nel caso specifico di eXtensiveControl®, le stringhe vengono utilizzate per imporre delle condizioni sui filtri, ma più in generale si tratta di trovare una corrispondenza attraverso una stringa campione (pattern) all'interno di un testo (o stringa) da analizzare. Per quanto riguarda la posta elettronica, si tratta di trovare una corrispondenza all'interno del messaggio o di un header dello stesso.

Si consideri ad esempio la necessità di esprimere una regola che blocchi l'utente *user01* appartenente al dominio *example.com*. Tale condizione può essere espressa semplicemente digitando nell'apposito box *user01@example.com* e verificando ad esempio che il campo di applicazione sia il "from" del messaggio se si desidera imporre una condizione (ad esempio un divieto) sull'invio dei messaggi da parte di quell'utente specifico.

Le cose si complicano se però si vuole allargare il campo di applicazione di tale regola non ad un utente specifico ma a molti; per esempio agli utenti *userXX@example.com*, ove XX è un numero a 2 cifre che va da 01 a 99. Si desidera cioè applicare la condizione ai primi 99 utenti del dominio. Naturalmente si potrebbero imporre 99 condizioni, una per ogni utente, tuttavia questo modo di procedere è poco pratico e soggetto ad errori. Per esprimere queste condizioni si possono usare forme espressive più elastiche che consentono di definire degli insiemi in maniera più semplice e veloce.

- *Simple expression*: le simple expression prevedono l'utilizzo di due caratteri speciali, l'asterisco (*) e il punto interrogativo (*?*). Questi caratteri, detti meta−caratteri, hanno un significato particolare quando utilizzati in una stringa campione con cui cercare una corrispondenza nel testo. Il significato di questi caratteri è analogo a quello a loro dato in altri contesti ad esmepio il comando di shell DOS *dir*. In particolare, quando si usa l'asterisco, viene verificata la corrispondenza con qualunque insieme di caratteri, in altre parole può essere sostituita con una sequenza arbitraria di caratteri. Il punto interrogativo rappresenta invece un singolo carattere, quindi può essere sostituito con un carattere qualunque.

  Ad esempio:

user@example.com	la condizione è verificata se trova la stringa *user@example.com*. Notare che il confronto è case insensitive e quindi viene verificato anche *User@Example.com* così come *uSeR@eXaMpLe.CoM*.
user?@example.com	in questo caso la condizione è verificata se la stringa corrisponde a meno del carattere *?* che può essere sostituito da un qualunque carattere. Ad esempio la condizione è verificata per *user1@example.com*, *user2@example.com*, *user3@example.com*, ecc., ma non ad esempio per *user@example.com* o per *user10@example.com*.
user*@example.com	in questo modo invece la condizione è verificata se la stringa ha come prefisso *user* e come suffisso *@example.com*. Qualunque sequenza di caratteri fra il prefisso e il suffisso viene accettata. Ad esempio: *user1@example.com* ed anche *user10@example.com*, *user10@example.com*, *user100@example.com*, *user10_temporary_account@example.com*, ecc.

- Le *case sensitive simple expression* sono equivalenti alle *simple expression* ad eccezione del fatto che sono (come il nome stesso suggerisce) case sensitive, ossia viene fatta distinzione fra minuscole e maiuscole. Quindi ad esempio se il pattern di confronto fosse come nel primo punto del caso precedente *user@example.com* la corrispondenza è verificata per *user@example.com* ma non *User@example.com*.
- Le *regular expression* sono un argomento piuttosto complesso che necessita di una trattazione a parte ed esula dallo scopo di questo manuale di supporto. Esse consistono in un insieme di regole che permette di esprimere con una semplice stringa condizioni particolamente complesse.

  Esiste parecchio materiale sia sulla rete Internet sia in forma cartacea sulle regular expression per chi fosse interessato ad approfondire questo argomento. Sebbene in questo contesto non si desideri dare indicazioni specifiche in materia, è comqune consigliabile fare una prova digitando *regular expression* su uno dei tanti motori di ricerca disponibili al fine di avere maggiori informazioni a riguardo e farsi una idea più specifica dell'argomento.

Dettagli

Per default la stringa che viene digitata nel box associato alla condizione viene considerata una simple expression; se si desidera imporre una *regular expression* occorre utilizzare la sintassi

re{ ... }

ove al posto dei puntini viene inserita l'espressione vera e propria. Nel caso si desideri invece esprimere una *case sensitive simple expression* occorre utilizzare la sintassi

cs{ ... }

Seguono alcuni esempi di stringhe con il relativo significato:

re{user[0..9]+@example.com}	questa è una regular expression che permette di verificare una qualunque forma del tipo *userXXX@example.com*, ove al posto di XXX può comparire una qualunque sequenza di caratteri numerici (cioè da 0 a 9).
cs{user@example.com}	vale lo stesso discorso della prima simple expression, con la differenza che qui è importante distinguere fra minuscole e maiuscole. Quindi ad esempio è verificata *user@example.com* ma non *User@example.com*.

Da notare che tutte le stringhe vengono inserite in una sola riga, eventuali andate a capo sono da considerarsi solamente funzionali al layout del testo di questo help.

Capitolo 10. Funzionamento del modulo SMTP

In questa sezione vengono descritti il funzionamento e la configurazione del modulo SMTP.

Introduzione

Il modulo SMTP viene tipicamente impiegato in due situazioni:

- La rete è dotata di un mail server interno e si desidera applicare i filtri sul contenuto dei messaggii prima che la posta raggiunga il mail server interno.
- Anche se la rete non è dotata di un mail server interno, l'amministratore desidera comunque applicare i filtri sul contenuto della posta in uscita.

In entrambi i casi è necessario avere un server esterno che faccia il relay della posta, ossia un mailer esterno di riferimento a cui i messaggi diretti ad utenti esterni vengono mandati per essere poi instradati verso destinazione.

Utilizzo con un mailer interno

Tipicamente quando la rete è dotata di un mail server interno, il ruolo di eXtensiveControl® è quello di filtrare la posta sia in entrata che in uscita. L'esempio in questione presuppone che la rete sia dotata anche di un firewall posto sul perimetro, che prima dell'installazione e configurazione di eXtensiveControl® ridirige la posta in ingresso (sull'indirizzo pubblico) verso il mail server (solitamente attraverso un meccanismo di forwarding della porta). Una corretta configurazione di eXtensiveControl® può essere la seguente:

- *Configurazione del firewall*: il dispositivo firewall che prima instradava la posta proveniente dall'esterno verso il mail server, viene ora configurato per mandare la posta a eXtensiveControl®, quindi alla coppia indirizzo/porta su cui è in ascolto il modulo SMTP.
- *Configurazione dei client*: i client potranno continuare a riceverela posta collegandosi con il protocollo POP3 al mail server, ma dovranno spedirla ad eXtensiveControl®. Sarà quindi necessario cambiare nei client il server in uscita e impostare la stessa coppia indirizzo/porta su cui il modulo SMTP di eXtensiveControl® è in ascolto.
- *Configurazione del mail server*: il mail server solitamente non necessita di alcuna modifica.
- *Configurazione del modulo SMTP di eXtensiveControl*®: Il modulo SMTP dovrà essere attivato e messo in ascolto su un indirizzo raggiungibile dalle altre macchine in rete (cioè non il localhost). Dovranno essere inoltre impostate le regole per impedire il relay non autorizzato (per maggiori informazioni vedere Capitolo 12, *Approfondimenti sul relay della posta via SMTP*).

  Occorre inoltre configurare il routing del MTA di eXtensiveControl® (per maggiori dettagli sul funzionamento del MTA vedere Capitolo 17, *MTA* o anche la sezione chiamata «Route»). In particolare bisognerà inoltrare verso il mail server interno i messaggi diretti agli utenti del dominio locale e verso l'esterno tutti gli altri.

  Per esempio, se il dominio interno è *example.com*, sarà necessario impostare il routing come segue:

example.com	indirizzo IP o nome del mail server interno
*	indirizzo IP o nome del mail server esterno di relay (server del provider)

  In questo modo se un messaggio è diretto al dominio interno (es. la destinazione è *user01@example.com* o *user0n@under.example.com*) viene girato sul server interno, mentre se è diretto all'esterno viene inoltrato al server di relay.

  È importante l'ordine con cui le regole di routing vengono inserite, perché la prima entry il cui dominio è verificato è quella che determina il routing. In altre parole se le entry della tabella di cui sopra fossero scambiate fra di loro, la prima regola (che sarebbe quella con "*") assorbirebbe tutti quanti i casi e tutta la posta sarebbe diretta all'esterno.

Utilizzo con un mailer esterno

In questo caso la configurazione è più semplice in quanto il modulo SMTP deve essere solamente interposto fra i client e il server esterno di relay. Nel dettaglio occorre:

- *Configurazione dei client*: i client dovranno spedire la posta attraverso il modulo SMTP di eXtensiveControl® e quindi collegarsi a quest'ultimo invece che al server di relay. Sarà quindi necessario cambiare nei client (ad es. Outlook Express) il server in uscita e impostare la stessa coppia indirizzo/porta su cui la componente SMTP di eXtensiveControl® è in ascolto.
- *Configurare il routing*: il modulo MTA di eXtensiveControl® dovrà essere configurato per instradare tutta la posta verso il server esterno (per maggiori dettagli sul funzionamento del MTA vedere Capitolo 17, *MTA* o anche la sezione chiamata «Route»).

  La tabella di routing conterrà quindi una sola regola, vale a dire:

*	<indirizzo IP del mail server esterno di relay>

Se si possiede un firewall, può essere utile, come misura di sicurezza, permettere l'accesso al server esterno soltanto alla macchina su cui è installato eXtensiveControl® e non ai singoli client che potrebbero quindi bypassare eXtensiveControl® semplicemente riconfigurando il client di posta.

Quando non si dispone di un server interno e si desidera filtrare anche la posta in ingresso, sarà necessario impostare tali filtri sul POP3, poiché senza un mail server interno, il modulo SMTP può essere utilizzato solo

per spedire la posta ma non per riceverla.

Capitolo 11. Modulo SMTP

Il modulo SMTP viene utilizzato per ricevere la posta, filtrarla e inoltrarla verso i mail server opportuni. Questa sezione contiene i dettagli relativi ai parametri di configurazione. Nel caso si desideri un'introduzione al funzionamento di tale modulo vedere Capitolo 10, *Funzionamento del modulo SMTP*

Info

La sezione Info presenta un riepilogo dello stato del modulo:

- Stato: Lo stato del modulo SMTP può essere: Disabilitato, Fermo, Avviato o In avvio.
- Data di avvio: Ultima volta che il modulo è stato avviato.
- Dimensioni file di log: Spazio occupato su disco dal file .log.
- Dimensioni file comandi processati: Spazio occupato su disco dal file comandi (estensione .lcd).
- Dimensioni file di debug: Spazio occupato su disco dal file con le informazioni di debug (estensione .err).

Ogni modulo, quando avviato, registra le informazioni relative al proprio funzionamento su tre file che portano il nome del modulo stesso ed estensioni (.log, .lcd e .err) dipendenti dal tipo di dati che raccolgono. Ogni giorno, ad un orario stabilito (che può essere variato a piacere) i file vengono rinominati e viene aggiunta la data corrente nel nome del file e poi viene creato un nuovo file senza data per il nuovo giorno. In questo modo i file si accumulano giorno per giorno e possono essere facilmente identificati dalla data che hanno nel nome stesso. Per default la rotazione avviene alle 23.58, quindi il file rinominato avrà la data corrente e tutte le informazioni relative a quel giorno (almeno fino alle 23:58) e gli ultimi 2 minuti del giorno precedente. In questo modo si otterranno dei file con riportata nel nome una data e all'interno di essi tutti i log relativi alla data indicata nel nome.

Nella parte inferiore della sezione è possibile accedere alle statistiche del modulo nell'ultima ora, giorno e settimana. Viene fornito un riassunto grafico delle attività del modulo, in modo da riconoscere immediatamente eventuali picchi di traffico, oltre al valore minimo, massimo e medio dell'attività visualizzata. Tipo specifica la caratteristica del modulo che si vuole visualizzare e Intervallo l'intervallo temporale che si desidera considerare nella statistica. Visualizza statistiche mostra le statistiche desiderate.

Avanzate

Significato dei parametri disponibili:

- Durata massima di una connessione: durata massima in secondi di una connessione. Un valore pari a 0 indica un tempo infinito
- Durata massima di una connessione inattiva: tempo massimo in secondi dopo il quale una connessione viene terminata se non arrivano dati dal server remoto
- Livello di debug: regola la quantità di log che viene generata dal modulo (file .err). Più piccolo è tale valore, minori sono le informazioni registrate. Tipicamente si incrementa il livello di debug in fase di diagnostica per capire la causa di un dato problema.
- Consenti host per cui non esiste il nome: può capitare che eXtensiveControl® debba eseguire una query DNS inversa da indirizzo IP a nome per applicare la politica di accesso definita nella sezione Regole di accesso. Questo accade ad esempio se si imposta una politica basata sui nomi delle macchine piuttosto che sui loro indirizzi IP. Se la conversione fallisce la connessione viene rifiutata a meno che questo flag non venga impostato.
- Relay da host locale: accetta di effettuare il relay se la mail proviene da una macchina che appartiene agli host locali.

- Permetti Relay da host esterni per domini locali: consente l'invio di mail aventi mittente appartenente ai domini locali da host esterni verso i domini locali.
- Accetta indirizzi incompleti (senza dominio): permette ad un messaggio proveniente da un utente che non specifica il dominio di essere accettato ugualmente e consegnato a destinazione.
- Indirizzo email a cui inviare gli avvisi: in caso vi sia la necessità di notificare l'amministratore, i messaggi in questione vengono inoltrati all'indirizzo ivi specificato.
- Numero massimo di linee di header nei messaggi di warning: Si tratta del numero di linee del messaggio originale che vengono riportate nel messaggio di warning (che riferendosi ad un altro messaggio, ne cita una parte).

Dopo avere cambiato la configurazione per salvare le modifiche è necessario premere il pulsante Salva. Il pulsante Annulla le modifiche effettua una rilettura della configurazione presente su disco rimuovendo le modifiche inserite e non ancora salvate.

Server

I server vengono utilizzati per associare ad un modulo uno o più indirizzi o porte di ascolto. Quando un client deve utilizzare un modulo per accedere ai servizi servizi forniti deve conoscere l'indirizzo e la porta TCP a cui connettersi per inviare le richieste. Tali parametri vengono configurati in questa sezione e sono specifici per ogni modulo. È importante fare attenzione all'utilizzo delle porte sulla propria macchina, poiché non è possibile permettere a due o più applicazioni di condividere la stessa coppia indirizzo/porta di ascolto. In particolare i moduli possono presentare dei malfunzionamenti qualora la coppia indirizzo/porta specificata come server sia già in uso da qualche altro processo. Se questo accade occorre cambiare i parametri associati al modulo, oppure le impostazioni dell'altro processo che crea il conflitto. Tipicamente il problema si risolve cambiando uno dei parametri in questione e riconfigurando i client che utilizzano quel servizio in modo da aggiornarli al cambiamento eseguito. Se è necessario cambiare un indirizzo IP ma la macchina ha una sola scheda di rete con un solo indirizzo IP associato, bisognerà aggiungere altri indirizzi alla scheda (e quindi alla macchina) attraverso le impostazioni di rete di Windows (sezione avanzate).

Il menu server presenta le seguenti azioni:

- Modifica: Permette di alterare una voce già inserita nella lista.
- Insersci: Permette di aggiungere una voce alla lista dei server. Ogni voce consiste in un indirizzo IP di ascolto e di una porta.
- Rimuovi: Permette di eliminare una voce dalla lista.
- Rimuovi tutto: Permette di eliminare tutte le voci dalla lista.

Regole di relay

Al fine di impedire utilizzi non autorizzati del motore SMTP di ricezione/trasmissione della posta elettronica, occorre fornire alcuni parametri che regolano l'accesso allo stesso. Una cattiva configurazione potrebbe portare a quello che è definito un open relay, cioè l'uso del servizio SMTP per spedire ad utenti esterni messaggi, tipicamente di pubblicità, non richiesti. Il vantaggio per costui consiste nel fatto che è la vostra macchina e non la sua a comparire come mittente (e questo gli permette quindi di celare la propria identità).

La sezione permette di impostare le regole di relay attraverso 4 sotto−sezioni:

- Domini interni: sono i domini per i quali il server accetta di fare da relay. Se il messaggio è diretto verso uno di questi domini esso verrà sempre consegnato. Se il messaggio proviene da uno di questi domini e l'indirizzo IP del mittente appartiene agli host locali, anche in questo caso il messaggio verrà instradato (qualunque sia la destinazione).
- Host locali: esprime l'insieme degli indirizzi IP locali, ovvero gli indirizzi IP della rete interna. E' possibile utilizzare la wildcard '*' per definire tale insieme: ad esempio 10.1.* definisce un insieme di

256x256 = 65536 indirizzi IP, tutti aventi prefisso 10.1.

- Controllo destinatari: è possibile impostare un filtro statico (con i dati su file), oppure un filtro dinamico attraverso il collegamento ad un dominio Active Directory (quest'ultimo utilizzabile solo con un server di posta Exchange) per bloccare messaggi indirizzati ad utenti del dominio interno non esistenti. Nel caso del file statico, è sufficiente indicare il path di un file che contiene la lista degli utenti (uno per riga) che il server deve accettare. Tutti gli altri vengono respinti. Nel caso di Active Directory con Exchange, occorre selezionare il dominio che interessa.
- Domini proibiti: domini da cui non si accetta posta (non è una vera e propria regola anti−relay, bensì una semplice blacklist). Si possono inserire indirizzi email oppure domini. Se si inserisce un dominio tutti gli indirizzi email che provengono dal quel dominio o da suoi sottodomini saranno rifiutati.

Notare che per ottenere un anti−relay efficace è necessario impostare sia i domini interni che gli host locali, in quanto una mail può avere falsificare il valore indicato come mittente ma l'indirizzo IP deve essere sempre valido.

Se si desidera avere maggiori informazioni su come configurare un server SMTP e sulle questioni legate al relay vedere Capitolo 12, *Approfondimenti sul relay della posta via SMTP*. Per aver informazioni sul collegamento di eXtensiveControl® con i domini Active Directory vedere Capitolo 15, *Collegamento ad Active Directory*

Filtro sulla posta

In questa sezione sono presenti tre sottosezioni principali. La sezione Avanzate parametrizza il comportamento dei filtri definendone dei parametri generici mentre le altre due definiscono i filtri applicati agli header e agli allegati. Ogni volta che arriva un messaggio viene prima applicato il filtro sugli header e poi quello sugli allegati.

Avanzate

La sezione Avanzate permette di definire dei parametri che modificano il comportamento dei filtri sugli header e sugli allegati. I parametri sono:

- Disabilita controllo sul path assoluto: talvolta capita che nel messaggio il nome dell'allegato contenga riferimenti (path) assoluti. Se questa voce viene abilitata, il messaggio viene lasciato passare anche se questo accade, altrimenti viene bloccato dal filtro sugli allegati senza che le regole di quest'ultimo vengano applicate. In altre parole il controllo sul path assoluto ha la precedenza sulle regole associate al filtro.
- Disabilita controllo sui nomi in Content−Type: esistono due campi per specificare il nome di un allegato nel formato MIME; se i due campi in questione sono in disaccordo, il messaggio viene lasciato passare solo se il box in questione è spuntato, altrimenti viene bloccato dal filtro sugli allegati prima di applicarne le regole.
- Numero massimo di estrazioni ricorsive negli archivi: indica fino a che livello di ricorsività estrarre gli archivi (ad esempio .zip) che contengono altri archivi, che contengono altri achivi, etc...
- Filtra anche il contenuto degli archivi: applica le stesse regole degli allegati anche al contenuto degli archivi. Per esempio, se si vietano le estensioni .doc, e se questa casella non è spuntata, un .doc all'interno di un file .zip non viene rilevato. Se tale opzione invece è attiva, allora il file viene riconosciuto.
- Blocca file crittati: Quarantena tutti gli allegati crittati, anche se contenuti in un archivio.

Filtro sugli header

Il filtro sugli header permette di eseguire determinate azioni in base al contenuto di header indicati.

Col pulsante Aggiungi è possibile inserire un numero a piacere di condizioni che dovranno essere tutte quante verificate affinché l'azione associata venga eseguita. Tali condizioni riguardano gli header del messaggio e sono:

- From (Header): è il mittente dichiarato negli header del messaggio ("From").
- To (Header): è il destinatario dichiarato negli header del messaggio nel campo "To".
- To o Cc: viene verificato il campo "To"("A") e "CC" ("CopiaConoscenza") del messaggio.
- Cc: campo "CopiaConoscenza" del messaggio.
- Subject: campo "Oggetto" del messaggio.
- Body: corpo del messaggio, comprende tutto quello che non è parte degli header.
- From: è il mittente dichiarato nella connessione SMTP.
- To: è il destinatario dichiarato nella connessione SMTP.
- Categoria link: verifica la presenza di link all'interno del messaggio relativi a siti di determinate categorie.
- Libero: se si seleziona questo campo sarà possibile digitare nel box che compare a fianco il valore di un header che si vuole filtrare.

Ogni sottosezione accetta tre tipi diversi di input, vale a dire delle *simple expression*, delle *regular expression* e delle *case sensitive simple expression*. Se si desiderano informazioni sulla sintassi di questi costrutti, oppure avere una panoramica generale delle stesse vedere Capitolo 9, *Pattern matching*

Le possibili azioni associate a questo filtro sono:

- Continua: vengono saltate le rimanenti regole e si passa al filtro successivo (che in questo caso è il filtro AntiVirus).
- Elimina: il messaggio viene eliminato.
- Permetti: il messaggio viene accettato e quindi viene inviato all'utente che sta scaricando la posta.
- Quarantena: il messaggio viene trasferito nella sezione quarantena "email bloccate" e dovrà essere gestito dall'amministratore, che deciderà se rilasciarlo o eliminarlo.

Se nessuna delle condizioni di questo filtro è verificata il programma passa all'analisi del filtro successivo, cioè quello degli allegati. Lo stesso accade se viene applicata l'azione "Continua".

Filtro sugli allegati

Permette di filtrare i messaggi in base al contenuto degli allegati. Una volta selezionata una regola si passa ad un pannello nel quale è possibile impostare oltre al "From" e al "To" una serie di condizioni ulteriori sul tipo di allegato. Da notare che il "From" e il "To" globali si riferiscono ai dati registrati dal modulo durante la connessione SMTP che ha inviato il messaggio e non a quelli dichiarati negli header. I pulsanti aggiungi e rimuovi permettono l'inserimento di queste condizioni. Ogni condizione può essere del tipo:

- From: la condizione è applicata al mittente del messaggio specificato durante la connessione SMTP.
- To: la condizione è applicata al destinatario del messaggio specificato durante la connessione SMTP.
- Nome dell'allegato: la condizione è applicata al nome del file allegato.
- Dimensione del messaggio: la condizione è applicata alla dimensione dell'intero messaggio; imponendo quindi un vincolo sulla sua dimensione e richiedendo che sia più grande o più piccolo di un determinato valore.
- Tipo dell'allegato: la condizione è applicata al tipo di file (apparirà a fianco una lista di tipi conosciuti). Il riconoscimento del tipo è basato su metodi euristici che analizzano la struttura interna del file.

Il filtro sugli allegati permette di effettuare le stesse azioni del filtro precedente (quello sugli header) e accetta la stessa forma di regular expression per la definizione delle regole.

Se nessuna delle condizioni in questa sottosezione viene verificata, il programma passa all'elaborazione del messaggio con il filtro successivo (in questo caso l'AntiVirus).

Antivirus

Il filtro AntiVirus permette di bloccare le mail contenenti virus worm o altro codice dannoso.

La sezione si compone di due sottosezioni: Generale ed Eccezioni. La sottosezione Generale è composta delle seguenti voci:

- Controllo AntiVirus: spuntare questa casella per abilitare il controllo AntiVirus. Se manca la spunta le rimanenti opzioni perdono di significato e vengono pertanto ignorate.
- Tempo massimo di scansione (sec.): se l'antivirus non restituisce una risposta entro il tempo specificato in questa casella, la mail viene considerata infetta.
- Azione sui messaggi infetti: Le azioni possibili su di un messaggio/allegato infetto sono le seguenti:
    - Quarantena e avvisa: Notifica l'amministratore che un dato utente ha ricevuto una mail virata e mette in quarantena il messaggio in questione.
    - Quarantena: Mette in quarantena il messaggio senza alcuna notifica.
    - Ritorna al mittente e avvisa: notifica l'amministratore che un dato utente ha ricevuto una mail virata e invia al mittente una notifica che il messaggio è stato bloccato.
    - Ritorna al mittente: Invia al mittente una notifica che il messaggio è stato bloccato senza avvisare l'amministratore.
- Comando AntiVirus (con path): in questo box occorre digitare il nome dell'eseguibile che deve essere lanciato da linea di comando per effettuare la scansione antivirus.
- Parametri del comando AntiVirus: in questo box è possibile digitare i parametri che si desiderano passare al comando antivirus quando viene avviata la scansione di un allegato.

La sottosezione "Eccezioni" permette di specificare uno o più domini o indirizzi email che saranno esclusi dal controllo antivirus quando indicati come destinatari nella sessione SMTP.

Se eXtensiveControl® rileva la presenza di un AntiVirus supportato riempie automaticamente i campi "Comando AntiVirus" e "Parametri del comando AntiVirus".

AntiSpam

La sezione si divide nelle seguenti sottosezioni:

- Generale: La sottosezione "Generale" si compone delle seguenti voci:
    - Controllo AntiSpam: questa casella determina se il filtro antispam è attivo. Se questa casella non è spuntata, il resto delle impostazioni nelle sezioni sottostanti perde di significato.
    - Azione sui messaggi di Spam: decide cosa fare quando viene rilevato un messaggio di spam (cioè quando viene rilevato uno punteggio di spam sopra la soglia impostata).
        - ♦ Marca il subject: contrassegna il subject del messaggio con la stringa presente nel box sottostante Marcatore dello Spam inserito nel Subject.
        - ♦ Quarantena: Sposta il messaggio nella quarantena. Sarà l'amministratore o gli utenti, se abilitati, successivamente a decidere se rilasciare o eliminare il messaggio.
        - ♦ Elimina: Scarta il messaggio senza notifica alcuna. È bene utilizzare questa opzione con cautela in quanto si rischiano di perdere dati importanti in caso di errore del filtro euristico.
    - Marcatore dello spam inserito nel subject: Nel caso l'azione associata al rilevamento Spam

indichi: "Marca il subject", la stringa che viene messa come prefisso nel subject del messaggio è quella presente nel box a fianco. Per default tale valore è "[SPAM]".
    - Soglia di Spam: identifica una soglia oltre la quale il messaggio è considerato spam. Il punteggio assegnato al messaggio dipende dai campioni forniti come training per il database.
- Whitelist: si tratta di una lista di domini o indirizzi di posta (considerati come mittenti) dai quale i messaggi vengono automaticamente riconosciuti come buoni con un peso di spam pari a 0 (il valore minimo).
- Blacklist: si tratta di una lista di domini o indirizzi di posta (considerati come mittenti) dai quale i messaggi vengono automaticamente riconosciuti come spam con un peso di spam pari a 100 (il valore massimo).
- Aggiornamento DB: questa sezione è un collegamento alla sezione Symbolic DB all'interno della voce AntiSpam della sezione Sistema e permette di effettuare un aggiornamento del database di spam, di pianificare il download in automatico e di configurare l'uso di un server proxy se è necessario per comunicare con Internet.

AntiPhishing

Questa sezione abilita il fitraggio antiphishing sulla posta gestita dal modulo ed è composta dalle seguenti sezioni:

- Generale:
    - Controllo AntiPhishing: questo checkbox abilita il controllo AntiPhishing.
    - Azione sui messaggi di Phishing: in questo campo è possibile definire le azioni da compiere sui messaggi ritenuti phishing. Le possibili azioni sono:
        - ♦ Marca il subject: contrassegna il subject del messaggio con la stringa presente nel box sottostante Marcatore del Phishing inserito nel Subject.
        - ♦ Quarantena: Sposta il messaggio nella quarantena. Sarà l'amministratore o gli utenti, se abilitati, successivamente a decidere se rilasciare o eliminare il messaggio.
        - ♦ Elimina: Scarta il messaggio senza notifica alcuna. È bene utilizzare questa opzione con cautela in quanto si rischiano di perdere dati importanti in caso di errore del filtro euristico.
    - Marcatore del Phishing inserito nel subject: questo form permette di specificare il tag da inserire nel subject delle mail ritenute phishing nel caso nel campo precendente si sia scelta l'azione di marcare il subject.
- Aggiornamento DB: questa sezione è un collegamento alla sezione Symbolic DB all'interno della voce AntiPhishing della sezione Sistema e permette di effettuare un aggiornamento del database, di pianificare il download in automatico e di configurare l'uso di un server proxy se è necessario per comunicare con Internet.

Il tasto "Annulla le modifiche" legge la configurazione correntemente presente sul disco cancellando le modifiche inserite e non ancora salvate, mentre il tasto "Salva" scrive la configurazione presente a video sul file di configurazione.

Quarantena

La sezione di quarantena permette di gestire i messaggi che vengono bloccati e quarantenati da uno dei filtri applicati alla posta.

In questa sezione è possibile effettuare le seguenti azioni:

- Rimuovi tutto: elimina tutti i messaggi che sono stati messi in quarantena.

- Rimuovi tutti i messaggi infetti: cancella tutti i messaggi sicuramente infetti. I messaggi posti in quarantena dai filtri o per i quali il controllo antivirus non ha fornito il responso di sicuremente infetti non sono cancellati.

Sono presenti le seguenti sezioni:

- Email bloccate: Questa sezione mostra i messaggi che vengono messi in quarantena perché ritenuti infetti o perché bloccati dalle regole di filtraggio sugli header o sugli allegati. Le tre righe presenti permettono di cercare per: id del messaggio, coda di messaggi più recenti (mostra gli ultimi *n* messaggi, dove n viene inserito nel box a fianco) oppure mostra i messaggi ricevuti nelle ultime n ore.
- Spam/Phishing: Il funzionamento è analogo alla sottosezione Quarantena/Email bloccate con la differenza che questo deposito contiene i messaggi ritenuti Spam o Phishing.
- Email malformate: Il funzionamento è analogo alla sottosezione Quarantena/Antivirus eccetto che in questo caso contiene i messaggi malformati.

Visualizzatore Log

La sezione Visualizzatore Log è divisa in 3 sotto sezioni che hanno funzionamento analogo fra loro, cioè quella di permettere la visualizzazione dei dati registrati nei 3 diversi file di log generati.

- Log: mostra il contenuto del file di log dove vengono registrate le attività dei proxy, in particolare essi tengono traccia delle azioni svolte dai client. Il formato segue lo standard Welf, pertanto suddetti file possono essere utilizzati per compilare report non solo dal motore interno di eXtensiveControl® ma anche da programmi di terze parti che supportano il formato Welf.
- Comandi: questa sezione mostra il contenuto del file comandi; nel file comandi vengono registrate informazioni aggiuntive rispetto al file di log, che per motivi di compatibilità col formato Welf non possono essere inserite direttamente nel file di log.
- Debug: mostra il contenuto del file di debug. Questo file risulta particolarmente indicato per diagnosticare eventuali problemi di funzionamento del modulo. La quantità di informazioni registrate nel file dipende dal livello di debug impostato nel menu Avanzate. Più il livello di debug è alto, maggiori saranno le informazioni registrate nel file (ma anche lo spazio occupato su disco, mentre le prestazioni del sistema tendono invece a calare). Solitamente si alza il livello di debug quando si presentano problemi di funzionamento e il numero di informazioni con il livello di default risulta essere insufficiente.

Tutti e tre i pannelli presentano la medesima interfaccia che si compone di tre voci:

- Punto di inizio della lettura: Permette di stabilire da quale punto del file iniziare la visualizzazione. È possibile visualizzare il contenuto dall'inizio del file, dalla fine o a partire da una linea specificata dall'utente.
- Numeri di linee: Numero di linee che l'utente intende visualizzare. Ad esempio impostando tale valore a 10 e la visualizzazione a partire dalla fine del file, si otterranno le ultime 10 linee del file. Tipicamente questa è la scelta più comune in quanto spesso si vogliono visualizzare le linee in prossimità di un errore appena avvenuto e che si trova dunque nelle alla fine del file.
- Risoluzione dei nomi: Con questa impostazione gli indirizzi IP vengono risolti in hostname in modo da essere più esplicativi. Ad esempio l'amministratore potrebbe voler sapere su quali siti navigano i suoi utenti (e non accontentarsi degli indirizzi IP). Non sempre è possibile risalire al nome di un host conoscendone l'indirizzo IP.

Capitolo 12. Approfondimenti sul relay della posta via SMTP

Il problema del relay

Il modulo SMTP è stato concepito per filtrare la posta in base a determinati criteri specificati dall'utente e poi inviarla (routing) verso la destinazione desiderata. Un problema che si può verificare durante questo processo e al quale è necessario prestare la dovuta attenzione, è di evitare utilizzi indesiderati da parte di estranei.

Al fine di evitare che utenti esterni utilizzino il modulo SMTP per spedire messaggi indirizzati ad altri utenti esterni, è necessario configurare correttamente il modulo SMTP. L'utilizzo improprio dei relay di posta (e il modulo SMTP rientra in questa categoria) è il maggior veicolo di diffusione dello spam, dove il mittente cerca di nascondere la propria identità. In tal caso infatti il destinatario finale vede il messaggio provenire dal modulo SMTP e non dal vero mittente. Lo scopo che ci si prefigge nella configurazione del modulo è quello di impedire che faccia da relay in queste circostanze. Per fare ciò occorre configurare correttamente i parametri "Host Locali" e "Relay Domain".

Supponendo di avere un Mail Server interno, devono essere *accettati* i seguenti messaggi:

- il messaggio proviene dall'esterno ed è diretto ad uno degli utenti interni al dominio.
- il messaggio proviene dall'interno ed è diretto o ad uno degli utenti interni al dominio o ad un dominio esterno.

deve essere invece *vietata* la seguente condizione:

- il messaggio proviene dall'esterno ed è diretto ad un utente esterno al dominio locale.

Purtroppo a questo occorre aggiungere che il solo dominio di provenienza della mail non è sufficiente a stabilire se il mittente è un utente interno o esterno. Il problema risiede infatti nella struttura stessa del protocollo SMTP che non prevede di autenticare il mittente. Naturalmente in caso di mittente fasullo, una eventuale risposta sarebbe impossibile da consegnare, tuttavia il problema nel caso in oggetto è di stabilire se il mittente può o no mandare il primo messaggio.

Per questa ragione occorre verificare anche ove si trova il server (o il client) che spedisce la mail al modulo SMTP, in particolare se l'indirizzo IP di tale server appartiene o no agli host della rete locale. Una volta definita questa classe di indirizzi, il modulo può stabilire agevolmente se effettuare il relay o no della mail che riceve.

Esempi di configurazione

Verranno presi ora in esame un paio di scenari e verranno dati suggerimenti su come configurare il modulo SMTP.

Negli esempi che seguono viene utilizzata la classe 10.xx.xx.xx come classe di indirizzi privata.

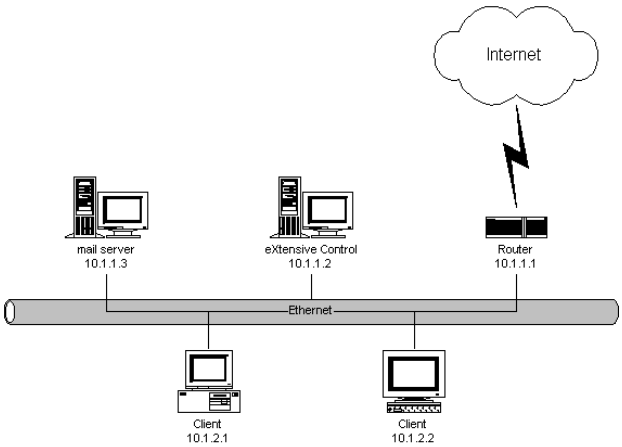
Configurazione del modulo all'interno di un firewall packet filter che fa NAT

Lo scenario si compone delle seguenti macchine:

- *Firewall Packet Filter che fa NAT* e inoltra la posta in entrata verso una macchina sulla rete interna
- *eXtensiveControl*® su cui è configurato il modulo SMTP per filtrare la posta
- *Sever di posta interno* che gestisce le caselle di posta degli utenti e a cui questi si collegano (tipicamente col protocollo POP3) per prelevare la posta.
- *Client sulla rete interna*: le macchine degli utenti che si collegano al server di posta per inviare e ricevere la posta.

Si supponga che il firewall abbia indirizzo interno (gateway) 10.1.1.1, eXtensiveControl® abbia indirizzo 10.1.1.2 e il server di posta 10.1.1.3. Tutti i client invece hanno indirizzi 10.1.2.xx, ove xx varia da client a client. Il dominio in cui gli account di posta sono definiti sarà *example.com* e gli utenti saranno user01, user02, ecc. Un indirizzo di posta valido sarà ad esempio *user02@example.com*.

Una possibile configurazione in questo caso è la seguente:



Ricezione della posta

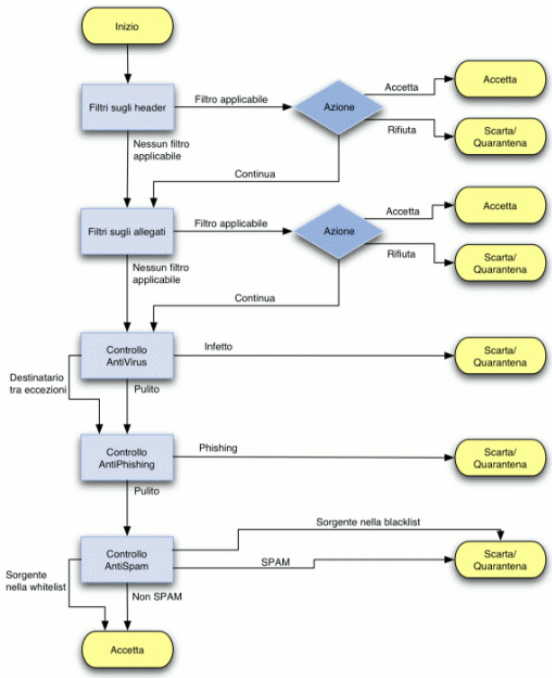
- Il firewall permette la connessione dalla sorgente esterna da cui la posta arriva verso il modulo SMTP di eXtensiveControl®, cioè verso il 10.1.1.2.
- Il modulo SMTP di eXtensiveControl® avrà configurato come relay domain: *example.com* e come host locale la classe *10.**. Inoltre, ma questo non fa parte delle regole antirelay, dovrà aver configurato la sezione Route del MTA (vedere la sezione chiamata «Route») per fare il relay di example.com verso il server interno di posta (10.1.1.3) e tutto il resto ("*") verso un server di relay esterno (oppure verso lo stesso server di posta 10.1.1.3 se è quest'ultimo che è preposto a spedire la posta verso il mondo esterno).
- Il server di posta verrà configurato per ricevere la posta solamente da eXtensiveControl® (quindi 10.1.1.2) in quanto i messaggi provenienti dai client dovranno passare attraverso quest'ultimo (in modo che possano essere all'occorrenza filtrati) prima di uscire verso l'esterno.
- I client dovranno invece essere configurati con l'impostazione SMTP (outgoing) che punta ad eXtensiveControl® cioè a 10.1.1.2.

Si osservi che quando la posta arriva dall'esterno, il firewall cambia solo l'indirizzo di destinazione (che in questo caso diventa il 10.1.1.2) ma non la sorgente, che figura quindi come esterna. Pertanto eXtensiveControl® accetterà di fare da relay solo per destinatari appartenenti al dominio *example.com*. Gli utenti interni, provenendo invece dalla classe 10.1.2.xx non avranno problemi a spedire la posta sia ad altri utenti interni sia ad utenti esterni, poiché il mittente ha dominio *example.com* e indirizzo appartenente all'insieme degli host locali.

Capitolo 13. Logica di filtraggio per le e–mail

Questa sezione illustra la logica con cui il motore di filtraggio opera sulla posta elettronica. Tale logica si applica, sebbene con qualche distinzione, sia al modulo SMTP che al modulo POP3.

In figura è mostrato lo schema di funzionamento del filtro:



come si può osservare sulla parte sinistra, il filtro sugli header, il filtro sugli allegati, il filtro antivirus, il filtro antispam e il filtro antiphishing sono applicati in sequenza. Se una regola impostata su uno dei filtri permette o nega la consegna del messaggio (con eventuale quarantena), allora l'azione viene eseguita e l'analisi termina. Se invece le regole di un dato filtro non trovano applicazione per un dato messaggio, l'analisi prosegue prendendo in considerazione il filtro successivo.

Fra le azioni possibili vi è anche quella di passare al filtro successivo in modo da saltare le condizioni che seguono nel filtro corrente. Infine alcuni filtri consentono dei percorsi alternativi, ad esempio il filtro antivirus permette di gestire una lista di eccezioni. Se il destinatario di un certo messaggio è fra le eccezioni, il messaggio non viene fatto passare attraverso il filtro antivirus e prosegue direttamente verso il filtro antiphishing.

Analogamente vi sono per il filtro antispam le whitelist e le blacklist che consentono di categorizzare la mail come spam o meno senza che il filtro bayesiano venga preso in considerazione. Anche in questo caso il messaggio non viene filtrato ma viene immediatamente classificato come ham o spam.

eXtensiveControl® permette di definire questi filtri nelle tre sezioni:

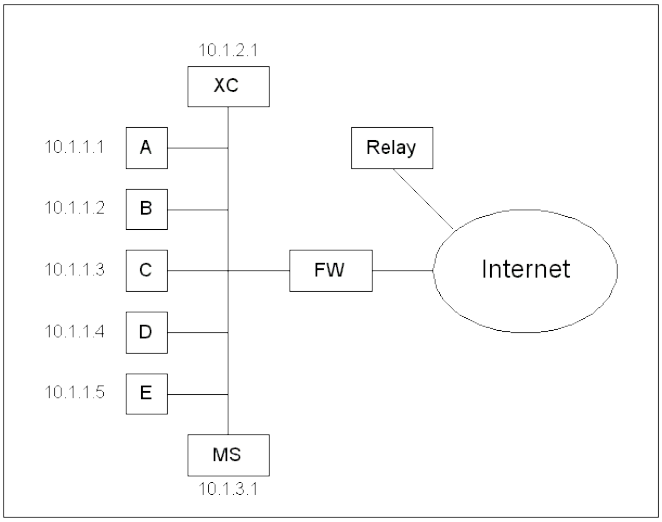
- *Filtro email* che si divide ulteriormente in *filtro sugli allegati* e *filtro sugli header*.
- *Antivirus*
- *AntiPhishing*
- *Antispam*

E' ovviamente importante tenere presente l'ordine di applicazione dei filtri quando si inseriscono le regole, perché il corretto funzionamento del sistema è principalmente una questione di precedenze.

Capitolo 14. Esempi utilizzo delle regole di accesso

In questa sezione verranno mostrati alcuni esempi pratici su come impostare le regole di accesso al fine di regolare la politica di naviagione e invio/ricezione posta degli utenti.

Nella figura sottostante è mostrata la struttura che verrà impiegata negli esempi che seguono. La rete è costituita da un firewall che implementa il Network Address Translation (NAT) e gestisce il traffico in entrata e in uscita. La rete interna ha classe di indirizzamento 10.1.0.0/16 e la struttura è dotata di un server mail interno, nonchè di un server di relay esterno che viene impiegato per spedire la posta.



Seguono ora alcuni esempi di regole per l'accesso alle risorse, suddivisi per tipologia, ovvero regole di accesso applicate alla navigazione WEB e regole di filtraggio per la posta.

Regole di accesso per il WEB

- *Esempio #1*. Si desidera garantire la navigazione libera a tutti ad eccezione della macchina A che non può navigare.

  Per impedire la navigazione alla macchina A è sufficiente anteporre una regola che vieta espressamente ad essa la navigazione (la macchina A avente indirizzo IP 10.1.1.1). Il risultato è mostrato nella tabella seguente:

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	10.1.1.1	*	Blocca	*	*
2	*	*	Permetti	*	*

  Quando una connessione viene ricevuta, il proxy web valuta se la prima regola è applicabile. Questo accade quando il requisito sulla sorgente è soddisfato ovvero se il client che si connette, ha indirizzo IP 10.1.1.1. Se la condizione è verificata, allora il proxy accetta la regola ed esegue l'azione associata, cioè rifiuta la richiesta della macchina A che viene pertanto bloccata.

  Se d'altro canto il client che si connette non è la macchina A, il vincolo non è soddisfatto e la regola viene saltata. Si passa dunque alla seconda regola che assorbe tutti gli altri casi e accetta tutto.

  Come risultato complessivo si ha che A non può navigare.
- *Esempio #2*. Oltre a bloccare la navigazione per la macchina A, si desidera impedire che le altre macchine, ad eccezione della macchina B (che è quella dell'amministratore), possano navigare su siti pornografici e sportivi.

  A parte mantenere la prima regola dell'esempio precedente (che blocca la macchina A), occorre inserire una seconda regola subito dopo che consente tutto alla macchina B. Notare che se B si connette al proxy, la regola #2 garantisce (essendo l'unico vincolo imposto sulla sorgente) che la regola venga applicata e che quindi l'host B abbia accesso indiscriminato al WEB.

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	10.1.1.1	*	Blocca	*	*
2	10.1.1.2	*	Permetti	*	*
3	*	cat: Pornografia, Sport	Blocca	*	*
4	*	*	Permetti	*	*

Per le altre macchine C,D ed E nessuna delle prime due regole può essere applicata, pertanto vi è la certezza che quando uno di questi tre client si collega, la regola C viene presa in considerazione. Ora tale regola viene applicata solamente quando il sito di destinazione è a contenuto pornografico o sportivo. Se questo accade allora l'azione associata viene eseguita e pertanto la connessione viene rifiutata.

Se neanche la terza regola può essere applicata, il che vuol dire che il sito non è nè a carattere pornografico nè a carattere sportivo, allora l'analisi passa alla quarta regola che permette tutto (il resto).

Il comportamento equivale dunque a quello richiesto dal quesito.

Notare in questo caso che non è stata fatta alcuna menzione esplicita nell'ACL delle macchine C,D ed E. Il riferimento infatti è ottenuto agendo per esclusione, ovvero le macchine A e B sono gestite dalle prime due regole rispettivamente. Tutto cioè che non è nè A nè B viene gestito dalle regole che seguono. Se si aggiungesse una quinta macchina F, anch'essa erediterebbe la stessa politica riservata alle macchine C,D ed E.

- *Esempio #3*. Rispetto all'esempio precedente, si vuole permettere la navigazione sui siti sportivi alle macchine C, D ed E durante il periodo di pausa che va dalle 13:00 alle 14:00 e fuori dall'orario di lavoro che comincia alle 8:00 e finisce alle 17:00. Rimane invece inalterata la politica di accesso per A e B.

  Il risultato richiesto lo si ottiene aggiungendo in terza posizione una regola che consente a tutti l'accesso ai siti sportivi negli intervalli di tempo permessi.

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	10.1.1.1	*	Blocca	*	*
2	10.1.1.2	*	Permetti	*	*
3	*	cat: Sport	Permetti	13:00−14:00, 17:00−8:00	*
4	*	cat: Pornografia, Sport	Blocca	*	*
5	*	*	Permetti	*	*

  Da notare che la regola #3 viene applicata solamente se il sito è a carattere sportivo e l'ora corrente cade in uno degli intervalli leciti. In altre parole i vincoli sulla destinazione e sull'intervallo temporale devono essere soddisfatti entrambi affinchè la regola venga applicata.
- *Esempio #4*. Cosa accade se dalla tabella nell'esempio precedente si rimuove l'ultima regola, cioè quella che permette tutto a tutti? Perchè si dice che tale regola permette tutto a tutti, se ad esempio ad A è espressamente vietato navigare?

  L'ultima regola per come è fatta assorbe tutto cioè che non è stato assorbito dalle regole precedenti. Se fosse la sola regola, allora in effetti permetterebbe tutto a tutti, ma essendo preceduta da altre regole, questa può permettere tutto solo a chi riesce a raggiungerla. A e B per esempio non possono mai raggiungerla a causa delle prime due regole che gestiscono appositamente tali macchine.

  Se viene rimossa l'ultima regola, ci sono delle situazioni in cui nessuna delle regole può essere applicata, in tal caso, esiste sempre una regola nascota che viene dopo tutte le altre, che gestisce tutti i casi non gestiti dalle regole espressamente inserite dall'amministratore e che blocca tutto.

  In altre parole è come se vi fosse come ultima regola invisibile quella che segue:

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	*	*	Blocca	*	*

  Naturalmente tale regola esiste solo al fine di rendere deterministico il comportamento del sistema, ovvero far sì che sia sempre definito il comportamento anche se le regole impostate dall'amministratore non coprono tutti i casi possibili. Nel tabella dell'esempio precedente tale regola

pur esistendo risulta irraggiungibile a causa della regola #5 che assorbe e permette tutto a tutti.

Se la regola #5 viene rimossa, il risultato finale è di permettere alle macchine C, D ed E la navigazione solo sui siti sportivi e solo negli intervalli al di fuori dall'orario di lavoro (cioè quelli espressi dalla regola #3).

Da notare inoltre che la regola #4 (l'ultima visibile dato che la #5 si è ipotizzato di rimuoverla) diventa a questo punto inutile, poichè chiunque superi la regola #3 non può comunque navigare.

- *Esempio #5*. Rispetto all'esempio #3, si desidera permettere alla postazione A di navigare dalle 10:00 alle 12:00 e si vuole vietare la pornografia anche a B (quindi a tutti).

  Per far questo è necessario inserire due regole in testa alla #1. La prima regola della nuova tabella ha il compito di vietare la pornografia a tutti, la seconda di permettere ad A di navigare nell'intervallo 13:00−14:00.

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	*	cat: Pornografia	Blocca	*	*
2	10.1.1.1	*	Permetti	10:00−12:00	*
3	10.1.1.1	*	Blocca	*	*
4	10.1.1.2	*	Permetti	*	*
5	*	cat: Sport	Permetti	13:00−14:00, 17:00−8:00	*
6	*	cat: Sport	Blocca	*	*
7	*	*	Permetti	*	*

  Da notare inoltre che è stato rimosso il vincolo della pornografia dalla regola #6 perchè ridondante. Infatti se l'utente tenta di accedere ad un sito pornografico, la regola #1 provvede a bloccarlo.

  Riassumendo la tabella in questo esempio mette in pratica le seguenti regole:

  - Nessuno può visitare siti pornografici.
  - *(A)* può navigare solo dalle 10:00 alle 12:00.
  - *(B)* può navigare ovunque eccetto che sui siti pornografici.
  - *(C, D e E)* possono visitare i siti sportivi solo fuori dall'orario di lavoro, ma possono navigare liberamente su tutti gli altri (ad eccezione dei siti pornografici) in qualunque ora del giorno.
- *Esempio #6*. Cosa succede se nella tabella dell'esempio precedente si rimuove la regola #3 che blocca A ?

  Il risultato è che A eredita gli stessi diritti delle macchine C, D ed E, con in più il privilegio di navigare su qualunque sito non pornografico dalle 10:00 alle 12:00. In altre parole A può visitare siti sportivi nell'intervallo 10:00 − 12:00, mentre a C,D ed E questo è permesso solo fuori dall'orario di lavoro (regole #5 e #6 nella tabella dell'esempio precedente).
- *Esempio #7*. In riferimento allo schema principale si vuole permettere la navigazione a tutti gli utenti, purchè si autentichino all'unico dominio (MyDomain) NT/2000 in uso.

  Prima di tutto è necessario verificare se vi è un gruppo del dominio che contenga tutti e solo gli utenti che si vuol far navigare. Per esempio il gruppo *Users* potrebbe essere adatto, in caso contrario sarà comunque sempre possibile crearne uno ad hoc e inserirvi gli utenti necessari.

  Il secondo passo è quello di impostare la regola relativa a tale gruppo. La tabella sottostante mostra una possibile soluzione:

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	*	*	Permetti	*	MyDomain/Users

Da notare che la corrispondenza sulla prima regola avviene solamente se l'utente fornisce uno username e password che stanno nella lista degli utenti "Users" del dominio. Cioè se l'utente è membro del dominio.

La regola nascosta entra in gioco qual'ora l'utente non fornisca le credenziali richieste in quanto se non vi sono le condizioni per effettuare una corrispondenza sulla prima regola, l'algoritmo che regola gli accessi passa ad analizzare la seconda regola (invisibile) che impedisce l'accesso a chiunque.

- *Esempio #8*. Cosa succede se nella tabella dell'esempio precedente si impone un vincolo nella sezione "Destinazione" che preveda solo siti di News ?

Accade che il gruppo User del dominio MyDomain può solo navigare sui siti di News e la navigazione è preclusa a tutti gli altri in qualunque sito, in virtù della regola nascosta.

- *Esempio #9*. Cosa succede se rispetto all'esempio precedente si inserisce come ultima regola un: "Permetti tutto a tutti" (vedi tabella sottostante) ?

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	*	cat: News	Permetti	*	MyDomain/Users
2	*	*	Permetti	*	*

Rispetto all'esempio precedente viene a mancare la regola nascosta perchè l'ultima regola visibile, di fatto, assorbe qualunque caso e impedisce che il sistema vada oltre e raggiunga la regola nascosta. In questo modo tutti gli utenti restano liberi di navigare dove desiderano.

Da notare che per come sono disposte le regole il sistema può alle volte chiedere all'utente di autenticarsi, ma se l'utente non fornisce i dati o fornisce dati non corretti, il sistema gli consente comunque l'accesso in virtù della seconda regola.

- *Esempio #10*. Sempre in riferimento allo schema principale si supponga che il dominio sia suddiviso nei gruppi "GruppoA", "GruppoB" e "GruppoC". I tre gruppi sono disgiunti, cioè ogni utente appartiene ad uno ed uno solo dei gruppi. Si desidera vietare agli untenti del GruppoA di visitare i siti sportivi e a quelli del GruppoB i siti di News. Tutto il resto è permesso.

Prima di tutto vediamo come *non bisogna fare* per risolvere questo problema. La tabella che seguen mostra un modo errato di impostare le regole:

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	*	cat: Sport	Blocca	*	MyDomain/GruppoA
2	*	cat: News	Blocca	*	MyDomain/GruppoB
3	*	*	Permetti	*	*

Sebbene queste regole sembrino sortire l'effetto desiderato, l'amministratore deve tenere conto che l'utente non è obbligato a fornire le credenziali e quindi autenticarsi. Pertanto se ad esempio un utente del gruppoA rifiuta di autenticarsi, il sistema gli consente, saltando oltre la prima regola, di navigare dove vuole. In altre parole la prima regola blocca l'utente del gruppoA solo se quest'ultimo gli fornisce le sue credenziali e si fa quindi riconoscere, ma non avendo una policy contro la navigazione anonima sui siti di News, il controllo è facilmente aggirabile.

Vediamo un secondo approccio che risolve il problema facendo leva sul fatto che i tre gruppi siano mutuamente disgiunti:

#	Sorgente	Destinazione	Azione	Intervallo temporale	Utente
1	*	cat: Sport	Permetti	*	MyDomain/GruppoB, MyDomain/GruppoC
2	*	cat: News	Permetti	*	

					MyDomain/GruppoA, MyDomain/GruppoC
3	*	cat: News, Sport	Blocca	*	*
4	*	*	Permetti	*	*

A differenza dell'esempio precedente, se un untente del gruppo A o del gruppo B rifiuta di autenticarsi, può comunque grazie alla regola #4 navigare liberamente ad eccezione dei siti di Sport e News per le quali la regola #3 impedisce a tutti l'accesso. Tuttavia se l'utente fa parte di un gruppo avente diritto di visitare una delle due categorie di siti ed accetta di autenticarsi, le regole #1 e #2 gli consentono l'accesso. Ad esempio un utente del gruppoB può navigare sui siti sportivi in base alla regola #1.

Regole di filtraggio per la posta

Per quanto riguarda la posta elettronica, le regole di accesso concepite come nel caso del web sono disponibili solo per il modulo POP3 e rivestono in ogni caso un ruolo di secondaria importanza. Il ruolo principale viene svolto dai quattro filtri: header, allegati, spam, phishings e antivirus.

Seguono alcuni esempi di impiego dei filtri.

- *Esempio #1*: si desidera attivare nel modulo SMTP solo i motori antispam, antiphishing e antivirus senza imporre alcuna restrizione sugli allegati ricevuti.

  Per fare questo è sufficiente abilitare il filtro antivirus, antispam ed antiphishing nelle relative sezioni; accertarsi che il filtro antivirus rilevi correttamente il path e i parametri da fornire al programma da linea di comando che verrà utilizzato per effettuare la scansione. Se questo non accade, fornire manualmente tali parametri.

  Per quanto riguarda l'antispam verificare che l'azione da intraprendere nel caso di rilevamento spam sia quella desiderata, vale a dire contrassegnare l'email oppure quarantenarla. E' possibile anche eliminarla direttamente, ma è altamente sconsigliato dal momento che il filtro non ha una accuratezza del 100% ed è per tanto possibile che agendo in tale modo qualche documento importante vada perduto.
- *Esempio #2*: rispetto all'esempio precedente si desidera evitare che la posta proveniente dal dominio *dominiosicuro.it* sia catalogata come spam, a prescindere dal contenuto e che venga invece considerato sempre come spam i messaggi provenienti da *spamfactory.com*

  E' sufficiente aggiungere il dominio *dominiosicuro.it* nelle whitelist e il dominio *spamfactory.com* nelle blacklist nella sezione antispam del modulo SMTP.
- *Esempio #3*: rispetto all'esempio precedente si desidera inoltre bloccare gli allegati contenenti programmi eseguibili a tutti gli utenti, mentre si desidera imporre un vincolo di 3Mb sulle dimensioni del messaggio, ad eccezione dei PDF e dei documenti di Office che possono passare anche se più grandi.

  Occorre impostare tre regole nella sezione allegati che nell'ordine:

  - *1*: vietino gli eseguibili (i divieti quando possibile vanno sempre messi prima dei permessi).
  - *2*: permettano file di tipo i .pfd e i documenti di Office.
  - *3*: vietino allegati di dimensioni maggiori di 3Mb.

  La tabella di regole risultante sarà pertanto la seguente:

#	From	To	Condizione	Azione	Commento
1	*	*	Se il tipo dell'allegato uguale a Eseguibili	Quarantena	

2	*	*	Se il tipo dell'allegato uguale a PDF;Documenti Microsoft Office	Continua	
3	*	*	Se la dimensione del messaggio >= 3M	Quarantena	

Da notare che nella seconda riga si è espressamente assegnato un permesso sui PDF e sui documenti di Office e non su un generico tipo documento che avrebbe incluso anche altri formati. Tale permesso è di tipo *Continua* e non di tipo *Permetti* in quanto quest'ultimo consentirebbe un accesso incondizionato ai documenti anche quando questi sono (ad esempio) virati.

Inoltre, in apparente contraddizione col suggerimento dato sopra, il vincolo sulla dimensione è stato inserito come ultimo dal momento che esso non deve valere sui PDF e sui documenti di Office.

Infine, vale la pena notare come, a differenza delle regole di accesso, qui non vi sia una regola nascosta in fondo che blocca tutto, dal momento che terminata l'analisi del filtro allegati, l'analisi passa al motore antivirus.

Per maggiori informazioni riguardo la differenza fra *Permetti* e *Continua* e più in generale sull'ordine di applicazione dei filtri, vedere Capitolo 13, *Logica di filtraggio per le e−mail*.

- *Esempio #4*: rispetto all'esempio precedente si desidera permettere al gruppo *support@example.com* di ricevere qualunque tipo di file in allegato, anche se virato (si presume che i tecnici di quel gruppo sappiano ciò che stanno facendo e che siano in grado di gestire i file infetti).

  E' sufficiente aggiungere una regola in testa che assegni un *Permetti* al gruppo in questione. Le tabella pertanto si modifica come segue:

#	From	To	Condizione	Azione	Commento
1	*	support@example.com	*	Permetti	
2	*	*	Se il tipo dell'allegato uguale a Eseguibili	Quarantena	
3	*	*	Se il tipo dell'allegato uguale a PDF;Documenti Microsoft Office	Permetti	
4	*	*	Se la dimensione del messaggio >= 3M	Quarantena	

Capitolo 15. Collegamento ad Active Directory

Introduzione Active Directory

Active Directory è un database gerarchico di risorse integrato nei domini Windows 2000 e Windows 2003. Il principale utilizzo è quello di conservare i riferimenti a risorse di vario tipo quali utenti, gruppi, cartelle condivise, stampanti, ecc. in un unico posto (dal punto di vista dell'amministrazione) in modo da poter reperire agevolmente le informazioni richieste.

Questo database contiene informazioni che possono essere utili ad eXtensiveControl® per gestire le policy dei proxy WEB e SMTP, in particolare nel database Active Directory sono memorizzati la lista degli utenti e dei gruppi appartenenti al dominio. Attraverso un collegamento col domain controller eXtensiveControl® può presentare una lista di utenti e gruppi che l'amministratore può utilizzare per comporre le regole di accesso.

eXtensiveControl® utilizza i dati estratti da Active Directory nelle seguenti circostanze:

- *Autenticazione WEB*: è possibile comporre le regole di accesso al WEB inerenti all'autenticazione utente, selezionando direttamente gruppi e utenti da una gui grafica piuttosto che doverli inserire manualmente. Per maggiori informazioni vedere la sezione chiamata «Regole di accesso»
- *Filtro sui messaggi (SMTP)*: se il mail server impiegato per la ricezione della posta è un server Exchange intergrato nel dominio Active Directory, è possibile utilizzare i dati del database per impostare un filtro che respinga tutte le mail indirizzate ad utenti del dominio non esistenti.

In questo modo i messaggi (tipicamente di SPAM) che presentano destinatari fasulli non raggiungono nemmeno il server di posta (che normalmente è l'entità che li respinge), ma si fermano a monte sul filtro SMTP di eXtensiveControl®.

Collegamento del proxy SMTP con Active Directory

Il proxy SMTP, se viene abilitato il filtro su Exchange, interroga periodicamente il domain controller per aggiornare una cache locale che viene utilizzata per decidere se un particolare messaggio deve essere accettato oppure no.

Il tempo di refresh viene impostato per default a 1200 secondi (20 minuti), ragione per la quale occorrono mediamente 10 minuti (nel peggiore dei casi 20 minuti, nel migliore l'aggiornamento è di pochi secondi) prima che un ipotetico utente appena creato sul domain controller possa ricevere posta.

Se necessario il tempo di refresh della cache può essere alterato attraverso la sezione *Regole di relay*, sottosezione *Controllo destinatari*. Riducendo il tempo si ottengono ritardi inferiori nella acquisizione di eventuali cambiamenti, ma al tempo stesso si carica maggiormente il domain controller. Al contrario se i tempi vengono allungati, il domain controller viene interrogato e quindi vengono impiegate più raramente le sue risorse a discapito di una latenza maggiore nell'aggiornamento dei dati. Una eventuale modifica deve essere dunque ponderata in base alle necessità e alle risorse della rete in questione.

Configurazione manuale del collegamento ad Active Directory

Il configuratore provvede attraverso il wizard al rilevamento automatico o semi automatico della configurazione del dominio se si decide di collegare eXtensiveControl® a quest'ultimo. Esistono tuttavia situazioni in cui per effettuare il collegamento è necessario inserire dati manualmente; tipicamente queste circostanze sono provocate da una configurazione anomala della rete che richiede l'intervento diretto sui parametri di configurazione o comunque un sistema per aggirare il problema.

Nella sottocartella config della cartella di installazione è presente il file *LDAP.conf* che memorizza le impostazioni Active Directory rilevate dal wizard o successivamente modificate attraverso l'omonima sezione. La struttura di questo file è piuttosto semplice. Ogni dominio (per default ne viene richiesto soltanto uno) ha il nome DNS racchiuso fra parentesi quadre, e da lì segue una lista di parametri che definiscono le caratteristiche del dominio. Questi parametri sono:

- *DC*: nome DNS o indirizzo IP del domain controller (possono essere più di uno, distribuiti su altrettante righe). Se vengono trovati (o specificati manualmente) più domain controller i proxy provvederanno a contattarli secondo una politica di tipo *Round Robin* (uno dopo l'altro in modo circolare) passando a quello successivo ogni qualvolta il programma non ottiene rispota dal domain controller di riferimento. In questo modo viene garantita una certa tolleranza ai guasti se un domain controller dovesse essere temporaneamente non disponibile.
- *NetBiosName*: nome netbios del dominio
- *AccountName e AccountPassword*: contengono le credenziali cifrate dell'utente avente i diritti per fare le query sul domain controller che il programma utilizza per collegarsi al dominio Active Directory. Per modificare questi valori occorre utilizzare l'interfaccia grafica. In questo caso si è preferito privilegiare la sicurezza delle credenziali piuttosto che la praticità di avere i dati in chiaro diretamente modificabili con un editor di testo (ma che sarebbero anche facili da acquisire da un intruso).
- *Port*: porta di comunicazione (usata dal proxy SMTP per connettersi al domain controller). Per default è la 389.

Questo file viene letto all'avvio dai quei proxy che necessitano i dati per connettersi al dominio (per ora il proxy SMTP se viene attivato il filtro Exchange).

Collegamento ad Active Directory in situazioni particolari

Quando eXtensiveControl® viene installato su una macchina appartenente ad un dominio, un eventuale collegamento ad Active Directory viene di norma effettuato in modo automatico una volta forniti i parametri richiesti (nome del dominio e credenziali per il collegamento). Esistono casi in cui questo non è immediato, da una parte se la macchina è fuori dal dominio, occorre fornire anche l'indirizzo di un domain controller, ma possono verificarsi anche casi più difficili, come quando eXtensiveControl® viene collocato in una DMZ e a separare il domain controller dal programma è un firewall che lascia passare solo determinate porte.

Tale situazione potrebbe ad esempio verificarsi se si desidera utilizzare eXtensiveControl® solo come filtro a monte per la posta e non si è interessati al controllo sulla navigazione.

In questi casi è fondamentale permettere il passaggio della porta LDAP (389) verso il domain controller (nell'esempio citato quindi dalla DMZ verso la rete interna), del servizio DNS e configurare le impostazioni Windows della macchina su cui è installato eXtensiveControl® per poter accedere a tale servizio.

Inoltre dovrà essere impostato un gateway opportuno se il firewall effettua una traslazione di indirizzi di rete (NAT), oppure dovrà essere possibile raggiungere il domain controller attraverso il forwarding di una porta. In ogni caso dovranno essere forniti i parametri per poter raggiungere i domain controller nella rete interna.

Capitolo 16. DNS

Il modulo DNS presente in eXtensiveControl® (Littlename) funge da cache DNS, esso viene utilizzato per velocizzare la risoluzione dei nomi dai moduli SMTP, POP3 e WEB. A partire dalla versioen 2.0 di eXtensiveControl® il modulo DNS è disattivato nelle nuove installazione. In condizioni normale non è necessario attivare questo servizio.

Info

La sezione "Info" presenta un riepilogo dello stato del DNS:

- Stato: lo stato del DNS può essere: Disabilitato, Fermo, Avviato o In avvio.
- Dimensioni file di log: spazio occupato su disco dal file .log.

Avanzate

La sezione Avanzate permette di definire il comportamento del DNS. Il significato dei parametri disponibili è il seguente:

- Indirizzo di ascolto: è l'indirizzo da cui la cache DNS ascolta per ricevere le richieste da inoltrare verso uno o più server DNS. La porta di ascolto di default è la 53 UDP.
- Porta locale di invio: indica la porta UDP dalla quale viene emessa la query verso il server remoto. Il valore 0 indica che la porta è dinamica, ovvero che è il sistema operativo a sceglierla nel momento in cui la query viene effettuata. Normalmente il numero di questa porta è irrilevante e pertanto è bene lasciare al sistema operativo la scelta, tuttavia esistono situazioni in cui può essere opportuno utilizzare una porta fissa (ad esempio nel debugging di una rete in modo da agevolare le operazioni di uno sniffer).
- Rispetta "Authoritative Flag": è un parametro strettamente legato al protocollo di risoluzione dei nomi. Per migliorare l'efficienza del sistema di distribuzione delle informazioni, i server DNS oltre a gestire i domini di loro competenza, sono in grado di interrogare altri server per fornire risposte a query su dati non in loro possesso. Inoltre un sistema di caching permette di velocizzare risposte a query che sono già transitate per quel particolare server. È detta *authoritative answer* una risposta

fornita direttamente dal server a cui quella particolare informazione fa capo; in altre parole se il client contatta direttamente il server e richiede un'informazione facente capo a tale server, quest'ultimo emette una risposta autorevole. Viceversa se l'informazione richiesta non è di pertinenza del server contattato, quest'ultimo può comunque fornire la risposta (perché ad esempio l'ha in cache o perché provvede lui stesso a contattare il server responsabile), tuttavia la risposta in tal caso è detta non autoritativa. Nel caso di Littlename, per default le risposte sono sempre non autoritative dal momento che esso è solo una cache e non è responsabile per nessun dominio. Spuntando la casella è tuttavia possibile renderlo trasparente, ovvero far si che l'autorevolezza o meno della risposta dipenda dal server che Littlename ha contattato, come se il client avesse contattato direttamente quel server.

- Aumenta il livello di debug: aumenta la quantità di informazioni emesse sul file di log.
- Usa connessioni TCP consente di utilizzare anche il TCP (e non come per default solo UDP) per instradare query verso i server DNS di riferimento (sezione forwarder). In questo caso, all'avvio del DNS, Littlename ascolterà anche sulla porta 53 TCP e contatterà sulla stessa porta i server remoti.
- Permetti il "Zone Transfer": definisce se è possibile effettuare un Zone Transfer tramite il protocollo TCP. Questa impostazione è irrilevante se non è stata spuntata la casella Usa connessioni TCP.
- Server per il "Zone Transfer": è la lista di indirizzi IP (separati da *:*) dai quali verrà accettata una richiesta di Zone Transfer. Ad esempio: *10.1.1.2:10.1.2.3:10.1.2.4* specifica che solo le macchine aventi uno dei tre indirizzi IP indicati potrà effettuare un Zone Transfer tramite Littlename.

Dopo avere cambiato la configurazione per salvare le modifiche è necessario premere il pulsante Salva.

Regole di accesso

Permette di impostare da quali indirizzi IP possono essere effettuate le query a Littlename. In questo modo è possibile permettere selettivamente solo a certe macchine di risolvere i nomi e proibire tale servizio a tutte le altre. Questa ACL consente di specificare l'insieme di indirizzi che possono accedere al servizio. Ogni entry specifica un indirizzo IP e una subnet mask. Quando la subnet mask è 255.255.255.255, allora la regola viene verificata solo se l'indirizzo IP corrisponde a quello del client chiamante. Specificando una subnet mask diversa è possibile invece indicare intervalli di indirizzi: per esempio un entry nella ACL del tipo: IP=10.1.2.3, subnet mask=255.255.255.0, consente l'accesso al servizio a tutte le macchine con indirizzi IP del tipo: 10.1.2.* (l'ultimo numero dell'indirizzo IP specificato è in questo caso irrilevante). Se la subnet mask fosse invece 255.255.0.0, il range di IP accettati sarebbe 10.1.* Naturalmente è possibile effettuare selezioni ancora più accurate settando opportunamente i valori della subnet mask.

Regole di inoltro

Tramite questa sezione è possibile stabilire verso quali server DNS sono indirizzate le query. LA scelta del server dipende dal contenuto della query stessa. Per esempio è possibile inoltrare tutte le richieste inerenti la risoluzione di nomi interni su di un server locale e passare a uno o più server esterni tutte le altre. È inoltre possibile specificare più server per una certa classe di domini, di modo che se il primo non è disponibile, automaticamente viene contattato il server successivo.

Nota

Quando si specifica più di un server per una data classe di domini, l'ordine con cui vengono contattati non è necessariamente dal primo all'ultimo poiché, al fine di ottimizzare i tempi sulle risposte alle query emesse, Littlename utilizza un algoritmo tipo round−robin che fa si che l'ultimo server che ha risposto sia messo come primo della lista per le successive query appartenenti a quella classe. In questo modo se ad esempio vengono specificati i server *A* e *B*, e per qualche motivo *A* non risponde, dopo il primo timeout/errore, *B* viene promosso a primo, fino a quando una richiesta non fallisce anche su di lui. In questo modo si evita che per ogni richiesta sia necessario attendere il timeout su *A* per poter risolvere un nome.

Ogni entry nel lista è composta da due campi:

- *Dominio*: è il dominio o la classe di domini per la quale si vuole impostare uno o più server. Il carattere @ viene utilizzato come carattere speciale per intendere qualunque dominio.
- *Server di riferimento*: è il server al quale si vuole inoltrare le query inerenti al domino o alla classe di domini specificati in *Dominio*.

Nota

Per ogni entry della lista è possibile specificare un solo *server*. Nel caso si vogliano impostare più server sarà necessario aggiungere nuove entry ripetendo lo stesso *Dominio*.

Zona locale

Si tratta di un sistema con cui è possibile forzare la risoluzione di determinati host con degli indirizzi IP stabiliti dall'amministratore (o viceversa). Infatti ogni volta che il DNS riceve una richiesta di risolvere un nome o un indirizzo effettua i seguenti passi:

- *Controllo della zona locale:* verifica se il nome è presente nella zona locale e in caso affermativo restituisce l'IP o il nome associato, altrimenti passa al punto seguente.
- *Controllo cache:* verifica se il nome è presente nella memoria cache e in caso affermativo restituisce il valore memorizzato, altrimenti passa al punto successivo.
- *Inoltro della richesta al server opportuno:* provvede ad inoltrare la richiesta al server di competenza per quel nome. Se dal server (o dai server, se sono più di uno) si ottiene una risposta prima di un tempo massimo, essa viene girata al client, altrimenti al client viene restituito un messaggio d'errore.

Come si può osservare, la zona locale ha la precedenza sull'eventuale risposta del server remoto, così che inserendo una copia nome/server come entry, è possibile ignorare la risposta del server (che pertanto non viene nemmeno interrogato) e forzare come risposta un determinato nome o indirizzo IP.

La zona locale è divisa in due sezioni a seconda dell'operazione di risoluzione che si desidera impostare:

- *Lista A:* viene utilizzata per impostare la risoluzione di determinati host coi relativi indirizzi IP.
- *Lista PTR:* viene utilizzata per impostare la risoluzione di determinati indirizzi IP coi relativi nomi di host.

Per ogni entry della zona locale è necessario definire un nome e un indirizzo IP o viceversa un indirizzo e un nome a seconda se si desidera forzare la risoluzione di un nome in un indirizzo o di un indirizzo in un nome rispettivamente.

Durante l'inserimento di una entry è possibile selezionare l'opzione Inserisci anche nell'altra lista, la quale inserisce l'entry sia per la conversione IP−nome (lista PTR) che per nome−IP (lista A).

Visualizzatore log

La sezione è composta da una sola sezione che permette di visualizzare il file di log della cache DNS scegliendo quante linee mostrare e il punto del file da cui partire per la visualizzazione.

I parametri di definizione della visualizzazione sono:

- Punto di inizio della lettura Permette di stabilire da quale punto del file iniziare la visualizzazione. È possibile visualizzare il contenuto dall'inizio del file, dalla fine o a partire da una linea specificata dall'utente.
- Numero di linee: Numero di linee che l'utente vuole visualizzare. Ad esempio impostando tale valore a 10 con l'inizio della lettura a fine file, si visualizzeranno le ultime 10 linee del file.

Oltre al tasto Visualizza per confermare i valori inseriti ed avere così la visualizzazione del log, è presente il tasto Scarica il file per salvare localmente tutto il file di log.

Capitolo 17. MTA

Descrizione

Il modulo MTA è il processo che si occupa di inviare le mail verso i server di destinazione. Viene utilizzato da eXtensiveControl® per diversi scopi:

- inviare le email ricevute ed analizzate dal modulo SMTP.
- inviare messaggi di notifica di qualora si dovessero verificare determinati eventi.
- rilasciare le mail quarantenate dal modulo SMTP.

È importante ribadire che se tale servizio non viene avviato ed ovviamente configurato correttamente, le operazioni elencate sopra non possono avere luogo.

Configurazione

Le sezioni necessarie alla configurazione sono solamente: Avanzate e Route. La configurazione di questo servizio è quindi molto più semplice rispetto a quella degli altri moduli e della cache DNS.

Info

La sezione Info presenta un riepilogo dello stato del modulo:

- Stato: Lo stato del modulo può essere: Disabilitato, Fermo, Avviato o In avvio.
- Data di avvio: Ultima volta che il modulo è stato avviato.
- Dimensioni file di log: Spazio occupato su disco dal file di log (estensione .log).
- Dimensioni file comandi processati: Spazio occupato su disco dal file comandi (estensione .lcd).
- Dimensioni file di debug: Spazio occupato su disco dal file con le informazioni di debug (estensione .err).

Ogni modulo, quando avviato, registra le informazioni relative al proprio funzionamento su tre file che portano il nome del modulo stesso ed estensioni (.log, .lcd e .err) dipendenti dal tipo di dati che raccolgono. Ogni giorno, ad un orario stabilito (che può essere variato a piacere) i file vengono rinominati e viene aggiunta la data corrente nel nome del file e poi viene creato un nuovo file senza data per il nuovo giorno. In questo modo i file si accumulano giorno per giorno e possono essere facilmente identificati dalla data che hanno nel nome stesso. Per default la rotazione avviene alle 23.58, quindi il file rinominato avrà la data corrente e tutte le informazioni relative a quel giorno (almeno fino alle 23:58) e gli ultimi 2 minuti del giorno precedente. In questo modo si otterranno dei file con riportata nel nome una data e all'interno di essi tutti i log relativi alla data indicata nel nome.

Avanzate

Nella sezione Avanzate sono presenti una serie di parametri che regolano il funzionamento del MTA.

- Livello di Debug: regola la quantità di log che viene generata dal MTA; più piccolo è il numero, meno informazioni vengono salvate. Escluse esigenze particolari, è consigliabile mantenere il valore di default.
- Sleep Time (sec): tempo che intercorre tra due attivazioni successive del processo per verificare se è presente della posta che deve essere spedita.

- Queue Time: tempo massimo che un messaggio può trascorrere in spool (cioè in coda in attesa di essere inviato) prima di essere rispedito al mittente.
- Spool warning time: tempo trascorso il quale, se il messaggio non è ancora stato recapitato, viene inviato un warning al mittente.
- Indirizzo email a cui inviare gli avvisi: indirizzo di posta elettronica a cui devono essere inviati i messaggi di warning.

Dopo avere cambiato la configurazione per salvare le modifiche è necessario premere il pulsante Salva.

Per rendere le modifiche effettive si deve far ripartire il servizio.

Route

La sezione *Route* serve per definire il routing per l'invio della posta. Per default il programma si comporta come gateway SMTP e pertanto si occupa solo di reindirizzare la posta verso altri server SMTP.

La sezione Route è composta da una lista di coppie <*Dominio*, *Server di riferimento*>, queste coppie indicano al MTA come eseguire il routing della posta, infatti esse specificano per ciascun dominio di posta il server di riferimento a cui inviare i messaggi. È possibile utilizzare il carattere speciale "*" per indicare qualunque dominio di posta.

Il modulo MTA esegue il routing in modo molto semplice; quando deve inviare un messaggio legge dal destinatario della mail il dominio a cui è destinata la mail, poi inizia a scorrere la lista partendo dal primo elemento (quello più in alto). Quando il primo elemento della coppia (*Dominio*) è un dominio padre o coincide con il dominio cercato il messaggio viene inviato al server di riferimento ad esso associato (si ricordi che "*" indica qualunque dominio). I messaggi per cui non è possibile determinare il server di riferimento non possono essere inviati.

Ad esempio con la seguente tabella di routing:

Dominio	Server
example.com	10.1.1.1
*	192.168.1.1

le mail inviate a user@example.com e user02@under.example.com sono indirizzate verso il server 10.1.1.1 mentre tutte le altre al server 192.168.1.1.

Visualizzatore log

La sezione "Visualizzatore log" è divisa in 3 sottosezioni che funzionano fra loro in modo analogo, cioè permettono la visualizzazione sul browser dei dati registrati dal MTA, anche se si applicano a tre tipologie di file differenti:

- Log: mostra il contenuto del file di log in cui vengono registrate le attività dei moduli, in particolare essi tengono traccia delle attività dei client. Il formato di output segue lo standard Welf, pertanto suddetti file possono essere utilizzati per compilare report non solo dal motore interno di eXtensiveControl® ma anche da programmi di terze parti che supportano il formato Welf.
- Comandi: questa sezione mostra il contenuto del file comandi dove vengono registrate informazioni aggiuntive, che per motivi di compatibilità con il formato Welf non possono essere inserite direttamente nel file di log in quanto il formato non lo prevede.
- Debug: mostra il contenuto del file di debug, dove vengono registrati gli eventi generati dal funzionamento del modulo MTA. Questo file risulta particolarmente indicato per tracciare il comportamento del software e diagnosticare eventuali problemi. La quantità di informazioni registrate nel file di debug dipende dal livello di debug impostato nel menu "Avanzate". Più il livello di debug è alto, maggiori saranno le informazioni registrate nel file (ma anche lo spazio occupato su disco,

mentre le prestazioni del sistema tendono invece a calare). Solitamente si alza il livello di debug quando si presentano problemi di funzionamento e il numero di informazioni con il livello di default risulta essere insufficiente.

Tutti e tre i pannelli presentano la medesima interfaccia che si compone di tre voci:

- Punto di inizio della lettura: Permette di stabilire da quale punto del file iniziare la visualizzazione. E' possibile visualizzare il contenuto dall'inizio del file, dalla fine o a partire da una linea specificata dall'utente.
- Numero di linee: Numero di linee che l'utente intende visualizzare. Ad esempio impostando tale valore a 10 e la visualizzazione a partire dalla fine del file, si otterranno le ultime 10 linee del file. Questa è la scelta più comune in quanto spesso l'utente vuole visualizzare le linee in prossimità di un errore appena avvenuto e che si trova dunque nelle ultime linee del file.
- Risoluzione dei nomi: Con questa impostazione gli indirizzi IP vengono risolti in nomi in modo da essere più esplicativi. Ad esempio l'amministratore potrebbe voler sapere su quali siti navigano i suoi utenti (e non accontentarsi degli IP).

Capitolo 18. Gestore della quarantena

Il gestore della quarantena si occupa della gestione di tutti i messaggi che si trovano nella quarantena del modulo SMTP siano essi bloccati perchè ritenuti spam o phishing, siano essi bloccati perchè virati o bloccati dai filtri in quanto in violazione della politica aziendale.

Il gestore permette la generazione periodica di messaggi riassuntivi di tutte le mail ferme in quarantena per tutti i destinatari dei messaggi. Periodicamente, quindi, ciascun utente riceverà una mail con tutti i messaggi ad esso relativi fermi in quarantena. L'utente potrà avere una visuale riassuntiva, oppure mediante un link accedere ad una sezione del configuratore in cui potrà avere una visione più dettagliata dei messaggi, ed eventualmente cancellarli o rilasciarli. Il rilascio è possibile solamente per le mail di spam/phishing.

È possibile poi definire una durata massima di un messaggio in quarantena, in questo modo le mail non si possono accumulare per più di un certo numero di giorni.

Report Spam/Phishing

Questa sezione permette di abilitare l'invio di una reportistica di tutti i messaggi fermi in quarantena perchè ritenuti spam/phishing. Tale reportistica viene inviata a tutti gli utenti che appartengono ad un dominio locale che hanno ricevuto dello spam e conterrà solamente i messaggi ad essi relativi. In questo modo tutti gli utenti potranno verificare la categorizzazione antispam/antiphishing applicata alla propria posta e potranno riconoscere e recuperare eventuali messaggi erroneamente bloccati.

Per abilitare questo report è necessario mettere i domini considerati locali nella configurazione del Modulo SMTP nella sezione Regole di relay Domini interni.

Il report inviato all'utente contiene una tabella dove ciascuna riga rappresenta un messaggio bloccato e per ciascuno di questi viene riportato mittente, soggetto e data di arrivo. Viene poi inviato un link che riporta ad una sezione del configuratore che permetterà di accedere in modo molto più dettagliato alle singole mail. Nella sezione di gestione del configuratore è anche possibile rimuovere i messaggi di spam/phshing e rilasciare i messaggi categorizzati in modo errato.

Stato

Questa sottosezione si occupa di riportare informazioni in merito all'operazione pianificata in oggetto.

- Risultato dell'ultima esecuzione: riporta lo stato di ritorno dell'ultima esecuzione dell'operazione pianificata, questa informazione è utile per determinarne il risulato e quindi rilevare eventuali malfunzionamenti.
- Ultima operazione eseguita: riporta la data e l'ora dell'ultima esecuzione.
- Prossima operazione : riporta la data e l'ora della prossima esecuzione.

Pianificazione

Questa sezione permette di attivare e configurare l'invio del report di quarantena.

- Abilita la reportistica: abilita l'invio del report ai singoli utenti.
- Periodicità del report: viene indicata la periodicità nell'invio del report. È possibile scegliere tra tre tipologie: giornaliera, giornaliera (feriale) e settimanale. La differenza tra "giornaliera" e "giornaliera (feriale)" consiste nel fatto che la prima viene eseguita ogni giorno, mentre la seconda ogni giorno escluso il sabato e la domenica. Se si seleziona l'invio giornaliero è possibile scegliere in quali orari eseguire l'invio, per introdurre un nuovo orario selezionare nelle finestre a scorrimento l'ora e i minuti del nuovo orario e poi premere su Inserisci. Per rimuovere un determinato orario, selezionare l'ora nel riquadro e poi premere Rimuovi. Per eliminare tutto premere Rimuovi tutto. Gli orari utilizzati per l'invio sono quelli presenti nel riquadro. Se si seleziona l'invio settimanale si dovrà scegliere in quale orario (in questo caso uno soltanto) eseguire l'invio e in quali giorni della settimana inviare i report. Per attivare il report è necessario scegliere almeno un giorno.

Email di report

Questa parte della configurazione permette di caratterizzare il messaggio di report che deve essere inviato. Le opzioni disponobili sono:

- Formato del messaggio: permette di definire il formato della mail di report, se in solo testo, in solo formato HTML o entrambi.
- Mittente della mail: indica il nome del mittente che verrà inserito negli header del messaggio che quindi sarà il nome che apparirà nel client di posta nel campo mittente.
- Soggetto della mail: rappresenta il subject del messaggio che verrà. In questo campo è possibile inserire delle macro per ottenere un soggetto estremamente descrittivo del contenuto della mail.
    - `$(UTENTE)` : indica il soggetto del report, cioè l'indirizzo di posta a cui è riferito il report.
    - `$(NUM)` : rappresenta il numero di mail presenti nel report.
    - `$(DATA)` : data di creazione del report.
- Inserisci un link per accedere all'area di quarantena: questo flag inserisce un link all'interno del messaggio che porta l'utente ad una sezione di gestione delle mail bloccate.
- Inserisci una tabella riassuntiva nella mail: il flag permette di inserire una tabella riassuntiva di tutte le mail bloccate.

Filtro

In questa sottosezione si può definire un filtro da applicare all'invio dei report di spam/phishing. In particolare è possibile scegliere chi riceverà il report e chi no, redirigere (redirect) il report relativo a determinati indirizzi di posta verso altri indirizzi. Il "redirect" può utile ad esempio quando si vuole definire un responsabile di un certo indirizzo di posta.

Per definire nuove regole di filtraggio è sufficiente premere su "Inserisci", a questo punto apparirà una finestra per la definizione della regola:

- Soggetto del report: definisce l'indirizzo di posta per cui è relativa questa regola.

- Operazione da intraprendere: definisce l'operazione da intraprendere con l'indirizzo appena inserito. Le possibilità sono: invia il report, non inviare il report, inoltra il report a.
- Destinatari della redirezione: questo campo appare solo se si sceglie inoltra il report a nel campo precedente. Questo form contiene l'indirizzo a cui inviare il report relativo all'indirizzo specificato nel campo Soggetto del report.

Nell'ultima riga è presente la scritta Tutti gli altri che indica l'azione da intraprendere per tutti quei soggetti non specificati nelle regole precedenti.

Report messaggi bloccati

Questa sezione permette di abilitare l'invio di una reportistica di tutti i messaggi fermi in quarantena perchè virati o bloccati dal sistema di filtraggio delle email. Tale reportistica viene inviata a tutti i destinatari delle email bloccate e conterrà solamente i messaggi ad essi relativi. In questo modo tutti gli utenti hanno la possibilità diverificare se dei messaggi sono stati bloccati.

Il report inviato all'utente contiene una tabella dove ciascuna riga rappresenta un messaggio bloccato e per ciascuno di questi viene riportato mittente, soggetto e data di arrivo. Viene poi inviato un link che riporta ad una sezione del configuratore che permetterà di accedere in modo molto più dettagliato alle singole mail. Nella sezione di gestione del configuratore è anche possibile rimuovere i messaggi, ma non rilasciarli per evitare che degli utenti rialscino per errore dei messaggi pericolosi.

Stato

Questa sottosezione si occupa di riportare informazioni in merito all'operazione pianificata in oggetto.

- Risultato dell'ultima esecuzione: riporta lo stato di ritorno dell'ultima esecuzione dell'operazione pianificata.
- Ultima operazione eseguita: riporta la data e l'ora dell'ultima esecuzione.
- Prossima operazione: riporta la data e l'ora della prossima esecuzione.

Pianificazione

Questa sottosezione permette di attivare e configurare l'invio del report di quarantena.

- Abilita la reportistica: abilita l'invio del report ai singoli utenti.
- Periodicità del report: viene indicata la periodicità nell'invio del report. È possibile scegliere tra tre tipologie: giornaliera, giornaliera (feriale) e settimanale. La differenza tra "giornaliera" e "giornaliera (feriale)" sta nel fatto che la prima viene eseguita ogni giorno, mentre la seconda ogni giorno escluso il sabato e la domenica. Se si seleziona l'invio giornaliero è possibile scegliere in quali orari eseguire l'invio, per introdurre un nuovo orario selezionare nelle finestre a scorrimento l'ora e i minuti del nuovo orario e poi premere su "Inserisci". Per rimuovere un determinato orario, selezionare l'ora nel riquadro e poi premere "Rimuovi". Per eliminare tutto premere "Rimuovi tutto". Gli orari utilizzati per l'invio sono quelli presenti nel riquadro. Se si seleziona l'invio settimanale si dovrà scegliere in quale orario (in questo caso uno soltanto) eseguire l'invio e in quali giorni della settimana inviare i report. Per attivare il report è necessario scegliere almeno un giorno.

Email di report

Questa parte della configurazione permette di caratterizzare il messaggio di report che deve essere inviato. Le opzioni disponobili sono:

- Formato del messaggio: permette di definire il formato della mail di report, se in solo testo, in solo formato HTML o entrambi.
- Mittente della mail: indica il nome del mittente che verrà inserito negli header del messaggio che quindi sarà il nome che apparirà nel client di posta nel campo mittente.
- Soggetto della mail: rappresenta il subject del messaggio che verrà. In questo campo è possibile inserire delle macro per ottenere un soggetto estremamente descrittivo del contenuto della mail.

    - `$(UTENTE)` : indica il soggetto del report, cioè l'indirizzo di posta a cui è riferito il report.
    - `$(NUM)` : rappresenta il numero di mail presenti nel report.
    - `$(DATA)` : data di creazione del report.
- Inserisci un link per accedere all'area di quarantena: questo flag inserisce un link all'interno del messaggio che porta l'utente ad una sezione di gestione delle mail bloccate.
- Inserisci una tabella riassuntiva nella mail: il flag permette di inserire una tabella riassuntiva di tutte le mail bloccate.

Filtro

In questa sottosezione si può definire un filtro da applicare all'invio dei report dei messaggi bloccati. In particolare è possibile scegliere chi riceverà il report e chi no, redirigere (redirect) il report relativo a determinati indirizzi di posta verso altri indirizzi. Il "redirect" può utile ad esempio quando si vuole definire un responsabile di un certo indirizzo di posta.

Per definire nuove regole di filtraggio è sufficiente premere su Inserisci, a questo punto apparirà una finestra per la definizione della regola:

- Soggetto del report: definisce l'indirizzo di posta per cui è relativa questa regola.
- Operazione da intraprendere: definisce l'operazione da intraprendere con l'indirizzo appena inserito. Le possibilità sono: invia il report, non inviare il report, inoltra il report a.
- Destinatari della redirezione: questo campo appare solo se si sceglie inoltra il report anel campo precedente. Questo form contiene l'indirizzo a cui inviare il report relativo all'indirizzo specificato nel campo Soggetto del report.

Nell'ultima riga è presente la scritta Tutti gli altri che indica l'azione da intraprendere per tutti quei soggetti non specificati nelle regole precedenti.

Rimozione

La sezione di Rimozione si occupa di pianificare la cancellazione automatica dei messaggi in quarantena, questa operazione è utile per evitare l'accumulo di messaggi.

In questa sezione si pianifica la rimozione automatica di messaggi più vecchi di un certo numero di giorni. Quotidianamente il sistema controllerà tutti i messaggi presenti nella quarantena eliminando quelli più vecchi del numero di giorni specificato. L'azione può essere eseguita selettivamente sulle mail di spam/phishing, bloccate e malformate. Se si inserisce 0 come numero massimo di giorni per cui un messaggio può stare in quarantena allora l'operazione viene disattivata.

Capitolo 19. Sistema

Informazioni

Questa sezione mostra alcuni parametri relativi al sistema che possono tornare utili sia in fase di configurazione sia durante la diagnostica di eventuali errori.

Sono riportate informazioni relative al sistema operativo, alla macchina che ospita il prodotto e alla versione dello stesso.

Il configuratore mostra tutte le partizioni presenti sul sistema, riportando per ciascuna di queste lo spazio disponibile e la dimensione totale.

Sono riportate anche tutte le schede di rete presenti sulla macchina e per ciascuna di queste sono indicati indirizzi IP (tutti quelli legati a quella particolare interfaccia di rete), server DNS e gateway.

Nella parte finale della pagina è possibile generare un report diagnostico con informazioni sul eXtensiveControl® e il sistema operativo presente. Nella prima riga viene indicato se è già presente un report (il summary) e quando questo è stato generato. Per aggiornare lo stato premere su aggiorna ora. Per scaricare localmente lo stato premere su scarica ora.

Qualora si dovesse presentare un problema si consiglia di aggiornare lo stato, scaricarlo localmente e poi inviarlo al supporto tecnico con una dettagliata descrizione del problema.

Categorizzazione WEB

Questa sezione è dedicata all'amministrazione del categorizzatore di siti (*cf_catmanager*). La funzione di questo servizio quello di caricare all'avvio i database richiesti per la categorizzazione dei siti (URL)e fornire le informazioni richieste ai modulo che ne hanno bisogno.

Dal menu Avanzate è possibile selezionare (oltre al livello di debug), quali database utilizzare. In particolare le scelte sono fra Nessuno, SurfControl, Open Source e BluePrint Data. In tutti e quattro i casi l'inclusione del database utente è implicita e viene effettuata automaticamente se l'utente ha provveduto a compilare un proprio database di siti.

Il servizio *cf_catmanager* viene automaticamente avviato dagli altri moduli se è necessario al loro funzionamento.

DB Utente

Questa sezione consente di gestire un database personale per la categorizzazione dei siti Web. In particolare l'amministratore ha a disposizione 10 categorie ognuna delle quali può contenere una lista di siti definibili da lui stesso.

Queste categorie possono essere utilizzate all'interno delle categorizzatore Web per definire in modo più flessibile i diritti di navigazione dei suoi utenti.

Ognuna delle 10 categorie (che nelle ACL vengono viste come UserDef01, ..., UserDer10) può contenere una lista di hostname lunga a piacere.

Per utilizzare questo databse è necessario eseguire la compilazione delle liste dopo aver inserito i valori. L'operazione di compilazione può essere effettuata facendo un clic su Compila. Lo stato della compilazione può essere visualizzato attraverso la voce Mostra i log di Compilazione.

Il pannello superiore mostra le 10 categorie utente e in ognuna di esse è possibile aggiungere, rimuovere o modificare la lista dei siti ivi contenuta.

La possibilità di inserire anche gli indirizzi IP nel database deve essere ponderata attentamente perché può portare ad effetti indesiderati. Uno specifico webserver (che ha uno o più indirizzi ad esso associati) può supportare più domini e di conseguenza imporre dei vincoli sull'IP significa alterare le regole di accesso in maniera imprevedibile. Se ad esempio uno stesso webserver gestisce sia siti pornografici che siti di interesse

generale, inibire il suo IP per impedire l'accesso ai contenuti pornografici, comporta quasi certamente l'esclusione anche di quelli di interesse generali dall'insieme dei siti accessibili.

Se si desiderano informazioni più generiche sul funzionamento del modulo WEB vedere Capitolo 5, *Funzionamento del modulo WEB*.

SurfControl® DB

Questa sezione gestisce gli aggiornamenti del database di categorizzazione web di SurfControl®. La pagina si compone di tre sezioni: Avanzate, Pianificazione e Stato.

Queste tre sezioni permettono di gestire l'aggiornamento del database di categorizzazione web di SurfControl®. La sezione Avanzate permette di definire le modalità di accesso alla rete, Pianificazione consente di pianificare l'aggiornamento mentre Stato mostra lo stato dell'aggiornamento.

Avanzate

In questa sezione è possibile definire l'uso di un eventuale proxy HTTP per comunicare con l'esterno.

Pianificazione

Questa sezione permette di definire un'operazione pianificata per aggiornare periodicamente il database. I parametri di configurazione sono:

- Abilita la pianificazione: permette di attivare o disattivare il download degli aggiornamenti.
- Ora di inizio: ora del giorno in cui l'aggiornamento viene eseguito.
- Periodicità della pianificazione: viene indicata la cadenza di esecuzione dell'aggiornamento. I possibili valori sono:
    - Giornaliera: l'operazione viene eseguita tutti i giorni all'ora specificata.
    - Settimanalmente: l'operazione viene eseguita ogni settimana all'ora specificata. Una volta scelta questa opzione apparirà sotto il parametro Giorno della settimana dove è possibile selezionare i giorni della settimana in cui eseguire il download.

Stato

Questa sezione mostra tutte le informazioni utili per determinare lo stato del Database e il suo aggiornamento.

- Ultimo aggiornamento corretto: riporta la data dell'ultimo aggiornamento del database andato a buon fine.
- Ultimo aggiornamento : riporta la data dell'ultimo aggiornamento del database indipendentemente dal risultato finale dello stesso.
- Stato dell'ultimo aggiornamento: riporta lo stato dell'ultimo aggiornamento
- Stato dell'aggiornamento manuale: Questa informazione è utile nel caso di aggiornamento manuale, viene riportato lo stato di un aggiornamento eseguito manualmente premendo il tasto aggiorna ora.

Nella parte bassa della tabella sono presenti tre pulsanti:

- Aggiorna ora: esegue un aggiornamento manuale del database.
- Mostra il file di log: mostra il file di log relativo alle operazioni di aggiornamento.
- Cancella DB: cancella il Database scaricato riportando il sistema nella situazione iniziale.

Open Source DB

Queste tre sezioni permettono di gestire l'aggiornamento del database di categorizzazione web Open Source. La sezione Avanzate permette di definire le modalità di accesso alla rete, Pianificazione consente di pianificare l'aggiornamento mentre Stato mostra lo stato dell'aggiornamento.

Avanzate

In questa sezione è possibile definire l'uso di un eventuale proxy HTTP per comunicare con l'esterno.

Pianificazione

Questa sezione permette di definire un'operazione pianificata per aggiornare periodicamente il database. I parametri di configurazione sono:

- Abilita la pianificazione: permette di attivare o disattivare il download degli aggiornamenti.
- Ora di inizio: ora del giorno in cui l'aggiornamento viene eseguito.
- Periodicità della pianificazione: viene indicata la cadenza di esecuzione dell'aggiornamento. I possibili valori sono:
    - Giornaliera: l'operazione viene eseguita tutti i giorni all'ora specificata.
    - Settimanalmente: l'operazione viene eseguita ogni settimana all'ora specificata. Una volta scelta questa opzione apparirà sotto il parametro Giorno della settimana dove è possibile selezionare i giorni della settimana in cui eseguire il download.

Stato

Questa sezione mostra tutte le informazioni utili per determinare lo stato del Database e il suo aggiornamento.

- Ultimo aggiornamento corretto: riporta la data dell'ultimo aggiornamento del database andato a buon fine.
- Ultimo aggiornamento : riporta la data dell'ultimo aggiornamento del database indipendentemente dal risultato finale dello stesso.
- Stato dell'ultimo aggiornamento: riporta lo stato dell'ultimo aggiornamento
- Stato dell'aggiornamento manuale: Questa informazione è utile nel caso di aggiornamento manuale, viene riportato lo stato di un aggiornamento eseguito manualmente premendo il tasto aggiorna ora.

Nella parte bassa della tabella sono presenti tre pulsanti:

- Aggiorna ora: esegue un aggiornamento manuale del database.
- Mostra il file di log: mostra il file di log relativo alle operazioni di aggiornamento.
- Cancella DB: cancella il Database scaricato riportando il sistema nella situazione iniziale.

BluePrint Data® DB

Queste tre sezioni permettono di gestire l'aggiornamento del database di categorizzazione web BluePrint Data®. La sezione Avanzate permette di definire le modalità di accesso alla rete, Pianificazione consente di pianificare l'aggiornamento mentre Stato mostra lo stato dell'aggiornamento.

Avanzate

In questa sezione è possibile definire l'uso di un eventuale proxy HTTP per comunicare con l'esterno.

Pianificazione

Questa sezione permette di definire un'operazione pianificata per aggiornare periodicamente il database. I parametri di configurazione sono:

- Abilita la pianificazione: permette di attivare o disattivare il download degli aggiornamenti.
- Ora di inizio: ora del giorno in cui l'aggiornamento viene eseguito.
- Periodicità della pianificazione: viene indicata la cadenza di esecuzione dell'aggiornamento. I possibili valori sono:

    - Giornaliera: l'operazione viene eseguita tutti i giorni all'ora specificata.
    - Settimanalmente: l'operazione viene eseguita ogni settimana all'ora specificata. Una volta scelta questa opzione apparirà sotto il parametro Giorno della settimana dove è possibile selezionare i giorni della settimana in cui eseguire il download.

Stato

Questa sezione mostra tutte le informazioni utili per determinare lo stato del Database e il suo aggiornamento.

- Ultimo aggiornamento corretto: riporta la data dell'ultimo aggiornamento del database andato a buon fine.
- Ultimo aggiornamento : riporta la data dell'ultimo aggiornamento del database indipendentemente dal risultato finale dello stesso.
- Stato dell'ultimo aggiornamento: riporta lo stato dell'ultimo aggiornamento
- Stato dell'aggiornamento manuale: Questa informazione è utile nel caso di aggiornamento manuale, viene riportato lo stato di un aggiornamento eseguito manualmente premendo il tasto aggiorna ora.

Nella parte bassa della tabella sono presenti tre pulsanti:

- Aggiorna ora: esegue un aggiornamento manuale del database.
- Mostra il file di log: mostra il file di log relativo alle operazioni di aggiornamento.
- Cancella DB: cancella il Database scaricato riportando il sistema nella situazione iniziale.

Utenti locali

Questa sezione permette di creare degli utenti e dei gruppi di essi localmente al software. Questi utenti vengono usati per l'accesso ai servizi Internet gestiti da eXtensiveControl®, in particolare per la navigazione web con autenticazione locale oppure per la generazione di report mirati al singolo utente dove verrà raccolto in un solo documento tutto il traffico web e di posta relativo allo specifico utente.

Utenti

In questa sotto−sezione è possibile creare nuovi utenti, modificare o rimuovere quelli esistenti. Ciascun utente avrà i seguenti campi:

1. Nome e Cognome dell'utente.
2. Account name associato all'utente, account che deve essere unico tra gli utenti, non vuoto e composto da lettere, numeri e dai caratteri di '.', '−' ed '_', quest'ultimi caratteri non possono essere il primo carattere dell'account.
3. Password.
4. Indirizzo di posta ad esso associato, qualora fossero presenti più indirizzi devono essere separati da una virgola.
5. Account di posta utilizzata dalla connessione POP3 per il download dei messaggi.
6. Commento.

Gruppi

In questa sotto−sezione è possibile creare nuovi gruppi, modificare o rimuovere quelli esistenti ed importare nuovi gruppi da file di testo esterni nella forma username spazio password. Ciascun gruppo avrà i seguenti campi:

1. Nome che deve essere unico tra i gruppi, non vuoto e composto da lettere, numeri e dai caratteri di '.', '−' ed '_', quest'ultimi caratteri non possono essere il primo carattere del nome.
2. Account utente che sono membri del gruppo.
3. Commento.

Il tasto importa da file legge un file importando i singoli utenti (qualora non fossero già presenti) creando così un nuovo gruppo.

Active Directory

Gestisce i parametri relativi al collegamento di eXtensiveControl® con uno o più domini Active Directory. Per informazioni riguardo al collegamento Active Directory vedere Capitolo 15, *Collegamento ad Active Directory*

AntiSpam

La sezione AntiSpam gestisce il motore anti−spam del prodotto. Qui è possibile gestire sia la parte di training dei messaggi campioni, che la verifica delle email inviate per essere utilizzate come campione.

Per capire meglio le sezioni Trainer, Archivio campioni ed Symbolic DB è necessario capire il funzionamento del motore antispam utilizzato all'interno del prodotto.

eXtensiveControl® verifica la presenza di spam utilizzando un filtro bayesiano, che assegna un punteggio alle email sulla base delle parole contenute, ciascuna parola avrà un peso diverso a seconda che sia più o meno probabile trovarla all'interno di una mail di spam piuttosto che in una mail buona (ham). Se il punteggio assegnato al messaggio supera una certa soglia definibile dall'utente la mail viene considerata spam. Il motore utilizza quindi un database di parole dove per ogni parola è associato un peso (che è legato alla probabilità di avere quella parola all'interno di un messaggio di spam e non di ham): questi pesi verranno utilizzati per assegnare un punteggio al messaggio. Ciò che permette al prodotto di operare in modo corretto è il database delle parole (o dei pesi); solo un database aggiornato consente di ottimizzare le operazioni di filtraggio. Questo database è composto in realtà da due database distinti uniti a formare un'unica base dati. Queste due parti sono il "Database Symbolic" e il "Database Utente" (che inizialmente sarà vuoto). L'uso del "Database Symbolic" permette all'amministratore del sistema di iniziare ad usare fin da subito il prodotto e minimizzare il tempo di gestione, infatti la sezione "Symbolic DB" permette di schedulare il download del db in modo da poter sempre avere un prodotto aggiornato ed operare al meglio. Il "Database Utente" permette un'ulteriore caratterizzazione del prodotto adattando le caratteristiche di questo al proprio traffico di posta.

L'operazione di aggiornamento del "Database Utente" avviene in due passi:

- Invio dei messaggi campione a eXtensiveControl®. L'inserimento può avvenire copiando le mail salvate su file in formato testo all'interno delle directory di deposito (sono indicate nella sottosezione Trainer come Directory di spam e Directory di ham) o inviandole mediante interfaccia grafica dalla sezione Inserimento spam nella schermata principale.
- Conferma dei messaggi inviati dalla sezione Inserimento spam mediante la sezione Archivio campioni.
- "Training", cioè lettura delle mail campioni presenti nel deposito e aggiornamento dei pesi nel databse delle parole.

La sezione Inserimento spam è importante perché consente anche a utenti che non possiedono diritti amministrativi sul prodotto di accedere al configuratore e inviare i propri campioni. Per evitare che vengano inviati dei campioni errati o piuttosto categorizzati in modo errato, i messaggi non vengono inviati al deposito definitivo ma ad un deposito temporaneo non interessato dal training, in cui l'amministratore ha la possibilità di accedere e di verificarli, confermarli spostandoli nel deposito definitivo, spostarli (da ham a spam o il contrario) o cancellarli. Queste operazioni sono eseguite nella sotto−sezione Archivio campioni.

Trainer

Questa sottosezione esegue l'operazione di training sui messaggi presenti all'interno del deposito definitivo. In questa sezione sono mostrati i percorsi delle cartella in cui si trovano i campioni di spam e ham. Viene inoltre ostrato lo stato del processo di training (che può essere in fase di esecuzione o inattivo) e il risultato dell'ultima operazione di training. L'ultima informazione riportata è relativa alla data di aggiornamento del database utilizzato nelle operazioni di antispam.

L'operazione di training è avviabile mediante il tasto Esegui il Training ed è possibile visualizzare i log relativi ai processi di training con il tasto Mostra il file di log.

Archivio campioni

In questa sezione è possibile accedere a tutti i messaggi inviati come campioni dalla sezione Inserimento spam. Le email sono divise in funzione della categoria Spam/Ham e per ciascun messaggio è possibile accedere al contenuto, rimuoverlo, spostarlo nell'altra categoria e confermarlo spostandolo nel deposito definitivo.

I messaggi presenti in questa sezione non vengono analizzati dalla fase di training.

Symbolic DB

Questa sezione gestisce gli aggiornamenti del database di categorizzazione delle mail di spam fornito da Symbolic. Com'è possibile notare la pagina si compone di tre sezioni: Avanzate, Pianificazione e Stato. Avanzate permette di definire le modalità di accesso alla rete, Pianificazione consente di pianificare l'aggiornamento, mentre Stato mostra lo stato dell'aggiornamento.

Avanzate

In questa sezione è possibile definire l'uso di un eventuale proxy HTTP per comunicare con l'esterno.

Pianificazione

Questa sezione permette di definire un'operazione pianificata per aggiornare periodicamente il database.

I parametri di configurazione sono:

- Abilita la pianificazione: permette di attivare o disattivare il download degli aggiornamenti.
- Ora di inizio: ora del giorno in cui l'aggiornamento viene eseguito.
- Periodicità della pianificazione: viene indicata la cadenza di esecuzione dell'aggiornamento. I possibili valori sono:

    - Giornaliera: l'operazione viene eseguita tutti i giorni all'ora specificata.
    - Settimanalmente: l'operazione viene eseguita ogni settimana all'ora specificata. Una volta scelta questa opzione apparirà sotto il parametro Giorno della settimana dove è possibile selezionare i giorni della settimana in cui eseguire il download.

Stato

La sezione mostra tutte le informazioni utili per determinare lo stato del Database e il suo aggiornamento.

- Ultimo aggiornamento corretto: riporta la data dell'ultimo aggiornamento del database andato a buon fine.
- Ultimo aggiornamento: riporta la data dell'ultimo aggiornamento del database indipendentemente dal risultato finale dello stesso.
- Stato dell'ultimo aggiornamento: riporta lo stato dell'ultimo aggiornamento
- Stato dell'aggiornamento manuale: viene riportato lo stato di un aggiornamento eseguito manualmente premendo il tasto aggiorna ora.

Nella parte bassa della tabella sono presenti tre pulsanti:

- Aggiorna ora: esegue un aggiornamento manuale del database.
- Mostra il file di log: mostra il file di log relativo alle operazioni di aggiornamento.
- Cancella DB: cancella il Database scaricato riportando il sistema nella situazione iniziale.

AntiPhishing

Questa sezione gestisce gli aggiornamenti del database di Phishing. È importante avere un db sempre aggiornato per poter bloccare il maggior numero di mail di phishing possibile e contrastare subito ogni nuova minaccia. Come è possibile notare la pagina si compone di tre sezioni: Avanzate, Pianificazione e Stato. Avanzate permette di definire le modalità di accesso alla rete, Pianificazione consente di pianificare l'aggiornamento, mentre Stato mostra lo stato dell'aggiornamento.

Avanzate

In questa sezione è possibile definire l'uso di un eventuale proxy HTTP per comunicare con l'esterno.

Pianificazione

Questa sezione permette di definire un'operazione pianificata per aggiornare periodicamente il database.

I parametri di configurazione sono:

- Abilita la pianificazione: permette di attivare o disattivare il download degli aggiornamenti.
- Ora di inizio: ora del giorno in cui l'aggiornamento viene eseguito.
- Periodicità della pianificazione: viene indicata la cadenza di esecuzione dell'aggiornamento. I possibili valori sono:
    - Giornaliera : l'operazione viene eseguita tutti i giorni all'ora specificata.
    - Settimanalmente: l'operazione viene eseguita ogni settimana all'ora specificata. Una volta scelta questa opzione apparirà sotto il parametro Giorno della settimana dove è possibile selezionare i giorni della settimana in cui eseguire il download.

Stato

La sezione mostra tutte le informazioni utili per determinare lo stato del Database e il suo aggiornamento.

- Ultimo aggiornamento corretto: riporta la data dell'ultimo aggiornamento del database andato a buon fine.

- Ultimo aggiornamento: riporta la data dell'ultimo aggiornamento del database indipendentemente dal risultato finale dello stesso.
- Stato dell'ultimo aggiornamento: riporta lo stato dell'ultimo aggiornamento
- Stato dell'aggiornamento manuale: Questa informazione è utile nel caso di aggiornamento manuale, viene riportato lo stato di un aggiornamento eseguito manualmente premendo il tasto aggiorna ora.

Nella parte bassa della tabella sono presenti tre pulsanti:

- Aggiorna ora: esegue un aggiornamento manuale del database.
- Mostra il file di log: mostra il file di log relativo alle operazioni di aggiornamento.
- Cancella DB: cancella il Database scaricato riportando il sistema nella situazione iniziale.

Gestione della Quarantena

Per informazioni riguardo la gestione della quarantena, vedere Capitolo 18, *Gestore della quarantena*

Licenze

La sezione Licenze permette di inserire i codici per l'attivazione del prodotto (il codice può essere introdotto anche durante la fase di installazione).

Capitolo 20. Report

La sezione reporter consente di creare dei report grafici in formato PDF contenenti le informazioni riguardanti il traffico generato dagli utenti.

Tale sezione si divide nelle seguenti sottosezioni:

- Report di sistema: questa sezione permette di generare un unico report, in cui vengono riportate le informazioni riassuntive sul traffico di rete e quelle più dettagliate sui singoli utenti e dei singoli host interni. Ciascuna sezione può essere disabilitata o parametrizzata a seconda delle esigenze. È possibile creare nuovi report manualmente o in modo pianificato, visualizzare quelli già presenti e cancellarli.
- Report per utente: questa sezione permette di generare un report per ogni utente, in cui verranno riportate le informazioni sul traffico di rete relativo a quel particolare utente. Anche questi report possono essere inviati via posta all'utente relativo. È possibile creare nuovi report manualmente o in modo pianificato, visualizzare quelli già presenti e cancellarli.
- Indirizzi locali: questa sezione serve per stabilire quali sono gli indirizzi da considerare interni alla rete e quali esterni. Questa distinzione ha rilievo, dal momento che il traffico viene diviso a seconda che sia dall'esterno verso l'interno (inbound) o viceversa: in più viene fornita una statistica delle macchine interne con maggior traffico e dei server esterni maggiormente contattati.

Report di sistema

La sezione Report di sistema permette di creare dei report relativi al traffico Internet dell'intera rete interna. Ciascun report è composto dalle seguenti sezioni:

- *Riepilogo generale:* mostra un riassunto di tutto il traffico, elencando prima i dati complessivi per poi classificarli per tipologia di traffico. Il fine di questa sezione è quello di fornire una visione d'insieme del flusso dati, mostrando gli host più attivi o i server più contattati, cioè tutte quelle informazioni che possano aiutare l'amministratore a capire il flusso dati.
- *Host:* vengono elencate tutte le macchine interne che hanno generato traffico. Per ciascuna di queste si riporta l'andamento medio del traffico per giorno della settimana e per ora del giorno e i server

maggiormente contattati.
- *Utenti:* sono riportati tutti gli utenti specificati nel report e per ciascuno viene mostrato il traffico web medio per settimana e per giorno, i siti maggiormente contattati e con cui c'è stato il maggior scambio di traffico. Qualora fosse legato all'utente anche uno o più indirizzi di posta verrebbero riportate le liste degli indirizzi a cui si spedisce maggiormente posta e di quelli da cui se ne riceve di più, oltre ad un grafico sulle tipologie di messaggi ricevuti (virus, spam o buone).

Il report generato può essere inviato via mail all'amministratore; l'esecuzione del report può essere fatta manualmente o pianificata mediante l'apposita sezione.

Archivio

Questa sezione mostra tutti i report di sistema archiviati localmente sulla macchina; è possibile creare manualmente un nuovo report, visualizzarlo o rimuoverlo.

Definizione di un nuovo Report

Questa pagina permette la creazione manuale di un nuovo report di sistema:

- *Generale:* Parametri generici per la definizione del report
    - *Descrizione:* qui è possibile inserire una breve descrizione sul contenuto dei dati del report.
    - *Salva report in archivio:* definisce se salvare il report nell'archivio una volta completato; può essere utile disabilitarlo se si vuole inviare il report via posta e non tenerne una copia localmente, in tutti gli altri casi si consiglia di lasciarlo abilitato.
    - *Invio tramite posta:* definisce se inviare il report via email, una volta abilitato questo flag appariranno altri form definire il destinatario, il mittente e il soggetto del messaggio.
    - *Crea il report più velocemente (alto utilizzo della CPU):* Permette di assegnare più risorse di calcolo alla creazione del report.
- *Filtro dei dati:* Definizione dei filtri per i log da analizzare
    - *Moduli da includere:* permette di scegliere quali moduli (quindi quale tipologia di traffico) includere nel report.
    - *Intervallo temporale di analisi:* Questo finestra a scorrimento è un supporto all'utente per la definizione dell'intervallo temporale di analisi definito dalle righe sottostanti. A seconda del campo scelto i valori si aggiorneranno automaticamente.
    - *Inizio lettura dati:* Definisce l'istante iniziale di analisi dei log, la data è nella forma giorno/mese/anno.
    - *Fine lettura dati:* Definisce l'istante finale di analisi dei log, la data è nella forma giorno/mese/anno.
- *Struttura del report:* Definizione del rendering del report
    - *Sezione 1 − Sommario > Abilita la sezione:* In questo tipo di report la sezione Sommario sarà sempre presente.
    - *Sezione 2 − Gli Host > Abilita la sezione:* Definisce se inserire la sezione degli Host all'interno del report.
    - *Sezione 3 − Gli Utenti > Abilita la sezione:* Definisce se inserire la sezione degli Utenti all'interno del report.
    - *Sezione 3 − Gli Utenti > Utenti da inserire:* Sono indicati gli utenti da inserire nella sezione Utenti. Per modificare questo valore è sufficiente cliccare su modifica. Subito sotto questa riga apparirà una finestra in cui è possibile scegliere gli utenti o i gruppi da inserire nel report. Come prima cosa si sceglie l'utente o il gruppo dal frame di destra, poi si preme su Inserisci(centralmente) in modo da confermare la selezione, questo sposterà l'utente o il gruppo nel frame di sinistra. Una volta terminata la selezione si preme su Conferma.

- *Configurazione generale > Conteggia dati solo per le utenze selezionate:* Nella sezione di riepilogo del report riport i dati aggregati considerando solo gli utenti scelti.
- *Configurazione generale > Includi primi n siti per traffico:* Vengono mostrati solo i primi n siti per traffico generato. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
- *Configurazione generale > Includi primi n siti per connessione:* Vengono mostrati solo i primi n siti per connessioni effettuate. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
- *Configurazione generale > Includi primi n siti bloccati:* Vengono mostrati solo i primi n siti bloccati a causa delle ACL. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
- *Configurazione generale > Numero n di siti da visualizzare:* Indica il numero di siti da mostrare per le opzioni precedenti se attivate.

Report Pianificati

Questa sezione mostra tutte le pianificazioni per la generazione dei report di sistema; è possibile crearne dei nuovi, modificarli o rimuoverli.

Definizione di un nuovo Report pianificato

Questa pagina permette la creazione di un nuovo report di sistema pianificato:

- *Generale:* Parametri generici per la definizione del report
    - *Descrizione:* qui è possibile inserire una breve descrizione sul contenuto dei dati del report.
    - *Salva report in archivio:* definisce se salvare il report nell'archivio una volta completato; può essere utile disabilitarlo se si vuole inviare il report via posta e non tenerne una copia localmente, in tutti gli altri casi si consiglia di lasciarlo abilitato.
    - *Invio tramite posta:* definisce se inviare il report via email, una volta abilitato questo flag appariranno altri form definire il destinatario, il mittente e il soggetto del messaggio.
    - *Crea il report più velocemente (alto utilizzo della CPU):* Permette di assegnare più risorse di calcolo alla creazione del report.
- *Pianificazione:* Parametrizzazione dello scheduling dell'esecuzione del report di sistema.
    - *Ora di inizio:* orario di esecuzione del report.
    - *Periodicità:* periodicità nell'esecuzione del report; può essere: giornaliera, giornaliera (feriale), settimanale, mensile. Se si sceglie settimanale apparirà una riga in cui selezionare i giorni della settimana in cui attivare la pianificazione. Se si sceglie mensile appariranno invece due righe, una per il giorno e una per il mese in cui attivare l'esecuzione.
- *Filtro dei dati:* Definizione dei filtri per i log da analizzare
    - *Moduli da includere:* permette di scegliere quali moduli (quindi quale tipologia di traffico) includere nel report.
    - *Intervallo temporale di analisi:* Questo finestra a scorrimento è un supporto all'utente per la definizione dell'intervallo temporale di analisi definito dalla riga sottostante. A seconda del campo scelto il valore si aggiornerà automaticamente.
    - *Durata dell'intervallo (giorni):* definisce il numero di giorni da considerare nel report a partire dall'istante di esecuzione, se ad esempio si scrive 5, si considerano gli ultimi 5 giorni dall'istante in cui si esegue il report. Il parametro *dalle/alle* indica l'ora iniziale e finale nella lettura dei log.
- *Struttura del report:* Definizione del rendering del report

- *Sezione 1 − Sommario > Abilita la sezione:* In questo tipo di report la sezione Sommario sarà sempre presente.
- *Sezione 2 − Gli Host > Abilita la sezione:* Definisce se inserire la sezione degli Host all'interno del report.
- *Sezione 3 − Gli Utenti > Abilita la sezione:* Definisce se inserire la sezione degli Utenti all'interno del report.
- *Sezione 3 − Gli Utenti > Utenti da inserire:* Sono indicati gli utenti da inserire nella sezione Utenti. Per modificare questo valore è sufficiente cliccare su modifica. Subito sotto questa riga apparirà una finestra in cui è possibile scegliere gli utenti o i gruppi da inserire nel report. Come prima cosa si sceglie l'utente o il gruppo dal frame di destra, poi si preme su Inserisci(centralmente) in modo da confermare la selezione, questo sposterà l'utente o il gruppo nel frame di sinistra. Una volta terminata la selezione si preme su Conferma.
- *Configurazione generale > Conteggia dati solo per le utenze selezionate:* Nella sezione di riepilogo del report riport i dati aggregati considerando solo gli utenti scelti.
- *Configurazione generale > Includi primi n siti per traffico:* Vengono mostrati solo i primi n siti per traffico generato. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
- *Configurazione generale > Includi primi n siti per connessione:* Vengono mostrati solo i primi n siti per connessioni effettuate. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
- *Configurazione generale > Includi primi n siti bloccati:* Vengono mostrati solo i primi n siti bloccati a causa delle ACL. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
- *Configurazione generale > Numero n di siti da visualizzare:* Indica il numero di siti da mostrare per le opzioni precedenti se attivate.

Report per utenti

La sezione Report per utenti permette di creare un report per ciascun utente specificato all'atto della creazione. Avere report separati è molto utile nel caso in cui si voglia inviare tali report agli utenti ad essi relativi, mantenendo così la riservatezza di tutti gli altri user. Ciascun report è composto dalle seguenti sezioni:

- *HTTP:* mostra il traffico web generato indicando l'andamento medio del traffico per giorno e per ora e le liste dei siti maggiormente contattati e di quelli con cui c'è stato il maggior traffico.
- *SMTP:* Se all'utente fosse legato uno o più indirizzi di posta, verrebbero qui riportate le liste degli indirizzi a cui si spedisce maggiormente posta e di quelli da cui se ne riceve di più, oltre ad un grafico sulle tipologie di messaggi ricevuti (virus, spam o buone). Questi dati vengo estratti dal Modulo SMTP.
- *POP3:* Se all'utente fosse legato uno o più indirizzi di posta, verrebbero qui riportate le liste degli indirizzi a cui si spedisce maggiormente posta e di quelli da cui se ne riceve di più, oltre ad un grafico sulle tipologie di messaggi ricevuti (virus, spam o buone). Questi dati vengo estratti dal Modulo POP3.

I report generati possono essere inviati via mail agli utenti relativi (se esiste un indirizzo associato ad essi); l'esecuzione del report può essere fatta manualmente o pianificata mediante l'apposita sezione.

Archivio

Questa sezione mostra tutti i report per utente archiviati localmente sulla macchina; è possibile creare manualmente un nuovo report, visualizzarlo o rimuoverlo. Qualora si volesse visualizzare un report apparirà una schermata intermedia in cui sono riportati i riport dei singoli utenti; per ciascuno di questi è possibile cancellarlo o visualizzarlo.

Definizione di un nuovo Report

Questa pagina permette la creazione manuale di un nuovo report per utenti:

- *Generale:* Parametri generici per la definizione del report
    - *Descrizione:* qui è possibile inserire una breve descrizione sul contenuto dei dati del report.
    - *Salva report in archivio:* definisce se salvare il report nell'archivio una volta completato; può essere utile disabilitarlo se si vuole inviare il report via posta e non tenerne una copia localmente, in tutti gli altri casi si consiglia di lasciarlo abilitato.
    - *Invio tramite posta:* definisce se inviare il report via email, una volta abilitato questo flag appariranno altri form definire il mittente e il soggetto del messaggio.
    - *Crea il report più velocemente (alto utilizzo della CPU):* Permette di assegnare più risorse di calcolo alla creazione del report.
- *Filtro dei dati:* Definizione dei filtri per i log da analizzare
    - *Moduli da includere:* permette di scegliere quali moduli (quindi quale tipologia di traffico) includere nel report.
    - *Intervallo temporale di analisi:* Questo finestra a scorrimento è un supporto all'utente per la definizione dell'intervallo temporale di analisi definito dalle righe sottostanti. A seconda del campo scelto i valori si aggiorneranno automaticamente.
    - *Inizio lettura dati:* Definisce l'istante iniziale di analisi dei log, la data è nella forma giorno/mese/anno.
    - *Fine lettura dati:* Definisce l'istante finale di analisi dei log, la data è nella forma giorno/mese/anno.
- *Struttura del report:* Definizione del rendering del report
    - *Report per utente > Utenti da inserire:* Sono indicati gli utenti per cui si deve creare il report. Per modificare questo valore è sufficiente cliccare su modifica. Subito sotto questa riga apparirà una finestra in cui è possibile scegliere gli utenti o i gruppi da inserire nel report. Come prima cosa si sceglie l'utente o il gruppo dal frame di destra, poi si preme su Inserisci(centralmente) in modo da confermare la selezione, questo sposterà l'utente o il gruppo nel frame di sinistra. Una volta terminata la selezione si preme su Conferma.
    - *Configurazione generale > Conteggia dati solo per le utenze selezionate:* Nella sezione di riepilogo del report riport i dati aggregati considerando solo gli utenti scelti.
    - *Configurazione generale > Includi primi n siti per traffico:* Vengono mostrati solo i primi n siti per traffico generato. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
    - *Configurazione generale > Includi primi n siti per connessione:* Vengono mostrati solo i primi n siti per connessioni effettuate. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
    - *Configurazione generale > Includi primi n siti bloccati:* Vengono mostrati solo i primi n siti bloccati a causa delle ACL. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
    - *Configurazione generale > Numero n di siti da visualizzare:* Indica il numero di siti da mostrare per le opzioni precedenti se attivate.

Report Pianificati

Questa sezione mostra tutte le pianificazioni per la generazione dei report per utente; è possibile crearne dei nuovi , modificarli o rimuoverli.

Definizione di un nuovo Report pianificato

Questa pagina permette la creazione di un nuovo report per utenti pianificato:

- *Generale:* Parametri generici per la definizione del report
    - *Descrizione:* qui è possibile inserire una breve descrizione sul contenuto dei dati del report.
    - *Salva report in archivio:* definisce se salvare il report nell'archivio una volta completato; può essere utile disabilitarlo se si vuole inviare il report via posta e non tenerne una copia localmente, in tutti gli altri casi si consiglia di lasciarlo abilitato.
    - *Invio tramite posta:* definisce se inviare il report via email, una volta abilitato questo flag appariranno altri form definire il mittente e il soggetto del messaggio.
    - *Crea il report più velocemente (alto utilizzo della CPU):* Permette di assegnare più risorse di calcolo alla creazione del report.
- *Pianificazione:* Parametrizzazione dello scheduling dell'esecuzione del report di sistema.
    - *Ora di inizio:* orario di esecuzione del report.
    - *Periodicità:* periodicità nell'esecuzione del report; può essere: giornaliera, giornaliera (feriale), settimanale, mensile. Se si sceglie settimanale apparirà una riga in cui selezionare i giorni della settimana in cui attivare la pianificazione. Se si sceglie mensile appariranno invece due righe, una per il giorno e una per il mese in cui attivare l'esecuzione.
- *Filtro dei dati:* Definizione dei filtri per i log da analizzare
    - *Moduli da includere:* permette di scegliere quali moduli (quindi quale tipologia di traffico) includere nel report.
    - *Intervallo temporale di analisi:* Questo finestra a scorrimento è un supporto all'utente per la definizione dell'intervallo temporale di analisi definito dalla riga sottostante. A seconda del campo scelto il valore si aggiornerà automaticamente.
    - *Durata dell'intervallo (giorni):* definisce il numero di giorni da considerare nel report a partire dall'istante di esecuzione, se ad esempio si scrive 5, si considerano gli ultimi 5 giorni dall'istante in cui si esegue il report. Il parametro *dalle/alle* indica l'ora iniziale e finale nella lettura dei log.
- *Struttura del report:* Definizione del rendering del report
    - *Report per utente > Utenti da inserire:* Sono indicati gli utenti da inserire nella sezione Utenti. Per modificare questo valore è sufficiente cliccare su modifica. Subito sotto questa riga apparirà una finestra in cui è possibile scegliere gli utenti o i gruppi da inserire nel report. Come prima cosa si sceglie l'utente o il gruppo dal frame di destra, poi si preme su Inserisci(centralmente) in modo da confermare la selezione, questo sposterà l'utente o il gruppo nel frame di sinistra. Una volta terminata la selezione si preme su Conferma.
    - *Configurazione generale > Conteggia dati solo per le utenze selezionate:* Nella sezione di riepilogo del report riport i dati aggregati considerando solo gli utenti scelti.
    - *Configurazione generale > Includi primi n siti per traffico:* Vengono mostrati solo i primi n siti per traffico generato. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
    - *Configurazione generale > Includi primi n siti per connessione:* Vengono mostrati solo i primi n siti per connessioni effettuate. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
    - *Configurazione generale > Includi primi n siti bloccati:* Vengono mostrati solo i primi n siti bloccati a causa delle ACL. Il parametro n è indicato dall'opzione Numero n di siti da visualizzare.
    - *Configurazione generale > Numero n di siti da visualizzare:* Indica il numero di siti da mostrare per le opzioni precedenti se attivate.

Motore di logging

Il servizio log_manager ha il compito di raccogliere gli eventi dai vari proxy e di scrivere i file di log nell'apposita cartella. Per evitare che i file nel tempo raggiungano dimensioni enormi, ogni giorno avviene la rotazione dei file e (a meno che non venga disattivata) la compressione degli stessi per ridurre lo spazio occupato.

Siccome di norma non è necessario alterare le impostazioni di default di log_manager, non vi sono comandi nell'interfaccia grafica atti allo scopo; in caso servisse tuttavia è possibile intevenire manualmente attraverso il file di configurazione *log_manager.conf* che si trova nella cartella config. Fare attenzione che evenutuali cambiamenti vengono letti solo all'avvio del servizio e poichè dal servizio log_manager dipendono tutti gli altri proxy, arrestare il log_manager implica che anche gli altri proxy vengano arrestati. Pertanto dopo aver modificato la configurazione sarà necessario riavviare non solo log_manager ma anche tutti i proxy che erano prima in funzione.

Ogni proxy durante il funzionamento produce attraverso log_manager 3 file nella cartella log che hanno come prefisso il nome stesso del proxy (es. Modulo_Web) e tre tipi di estensioni diversi a seconda del contenuto (vedere per esempio la sezione chiamata «Visualizzatore Log»). Ad una certa ora del giorno (per default le 23:58, ma modificabile attraverso il file di configurazione), i 3 file di log di ogni proxy vengono rinominati, compressi e nuovi file coi vecchi nomi vengono creati.

In questo modo per il modulo web, ad esempio, i 3 file *Modulo_Web.log*, *Modulo_Web.lcd* e *Modulo_Web.err* rappresentano sempre e comunque i file coi log più recenti.

Quando i file vengono rinominati, il nuovo nome prevede un suffisso con due date che definiscono i limiti temporali degli eventi stessi e servono quando si compila un report per permettere al programma di reperire più rapidamente i file che contengono gli eventi compresi nell'intervallo di reportistica selezionato.

Per esempio un file con nome: *Modulo_WEB.lcd.20090207235844−20090208235749.gz* sta ad indicare un file .lcd compresso il cui intervallo temporale degli eventi va dalla data e ora di inizio: 07/02/2009 23:58:44 alla data e ora di fine: 08/02/2009 23:57:49. Se venisse dunque richiesto un report che va dal 15 al 22 di febbraio 2009, il programma, visto il nome del file, salterebbe lo stesso evitando di sprecare tempo su eventi che non appartengono all'intervallo richiesto.

Il motore di reporting è in grado di leggere i file compressi, senza dover effettuare una copia temporanea decompressa, tuttavia qual'ora si ritenesse necessario rinunciare alla compressione automatica dei file durante la rotazione, è possibile impostare (o inserire) il parametro:

```
CompressOnRotation=0
```

Se il parametro viene omesso, equivale a impostarlo a 1 e quindi la compressione avviene. Notare quindi che se il prodotto viene aggiornato da una versione vecchia che non prevedeva la compressione, per default questa si attiva automaticamente, perchè l'installatore non modifica il file *log_manager.conf* durante l'aggiornamento e ovviamente nelle vecchie versioni questo parametro non c'era.

Capitolo 21. Configuratore

Questa sezione permette di cambiare le impostazioni del configuratore definendo in dettaglio le modalità di accesso al web server di configurazione e la definizione di nuovi utenti per le diverse parti che compongono il sito di configurazione di eXtensiveControl®

Le diverse parti che compongono questa sezione sono: Avanzate, Utenti del configuratore, Utenti dell'inserimento spam e Riavvio del configuratore.

Avanzate

In questa sottosezione è possibile definire le modalità di accesso al server di configurazione. I campi sono:

- Indirizzo di ascolto è l'indirizzo su cui il configuratore risponde alle richieste. Se questo indirizzo è il localhost (127.0.0.1) sarà possibile accedere all'interfaccia solo dalla macchina locale. Per permettere anche ad altre macchine di accedere al configuratore è necessario scegliere l'indirizzo di una scheda di rete raggiungibile dagli altri client. Occorr modificare in modo opportuno gli IP permessi quando si altera questo valore.
- Porta: La porta di ascolto del configuratore. Per default è la 8000.
- IP permessi: È la lista di indirizzi IP separati dal carattere *:* che hanno il permesso di accedere al configuratore. È possibile indicare anche un insieme di indirizzi IP utilizando la wildcard *.

  Ad esempio la seguente riga permette l'accesso ai client prefisso IP 10.1

  ```
  10.1.*
  ```

  mentre quest'altra riga permette l'accesso ai due host 10.1.1.1 e 10.1.1.2

  ```
  10.1.1.1:10.1.1.2
  ```

- Mostra il Traceback: è utile come diagnostico nel caso si verifichino certi tipi di errori. Potrebbe essere richiesto di abilitarlo dal personale del supporto tecnico in caso di necessità.
- Abilita SSL: serve per abilitare il protocollo SSL al fine di comunicare in modo protetto (mediante crittografia) con il configuratore. In questo modo è possibile permettere l'accesso al configuratore anche dall'esterno, garantendo comunque la sicurezza della connessione. Qualora non fossero presenti i certificati necessari per abilitare SSL, verranno richieste alcune informazioni per la loro generazione automatica.
- Password: permette di cambiare la password di accesso dell'utente amministrativo "admin".
- Conferma Password: box di conferma della nuova password (occorre digitare la stessa password inserita nel box Password.

Utenti del configuratore

Questa sezione permette di stabilire quali utenti possono accedere al configuratore di eXtensiveControl® oltre all'amministratore. L'amministratore può sempre accedere all'interfaccia attraverso lo user *admin* e la password che ha scelto durante l'installazione del prodotto (e che può modificare attraverso la sezione Avanzate).

Se viene tolta la spunta al checkbox Abilita l'autenticazione gli utenti hanno il permesso di accedere al configuratore senza che sia richiesta l'autenticazione. In caso contrario invece solo l'amministratore e gli utenti predefiniti possono modificare col browser le impostazioni del prodotto.

Il pannello inferiore consente di definire e quindi inserire (tasto Inserisci) l'utente. Selezionando invece un utente nel box di destra e facendo clic su Rimuovi è possibile rimuovere l'utente dalla lista di quelli abilitati ad accedere al configuratore.

Le opzioni Salva e Annulla le modifiche servono rispettivamente per scrivere o leggere da disco la configurazione, lettura che elimina tutte le modifiche inserite fino a quel momento e non ancora salvate.

Utenti dell'inserimento Spam

Questa sezione permette di selezionare chi può effettuare l'invio dei campioni di ham e spam attraverso l'interfaccia web. Gli utenti, se ne hanno i diritti, possono collegarsi direttamente all'uploader e attraverso il browser inserire nel deposito centralizzato i mesaggi di posta. Per default, tutti possono accedere a questa sezione ed inviare i propri campioni senza la necessità di alcuna autenticazione.

Le opzioni disponibili sono le seguenti:

- Abilita la sezione: se viene disabilitato, l'intera sezione di inserimento non sarà più accessibile, e tutte le opzioni che seguono perderanno di significato.
- Abilita l'autenticazione: se viene disabilitata tutti gli utenti avranno accesso all'uploader dei messaggi (a condizione che la sezione sia abilitata).
- Conferma ogni messaggio se l'autenticazione è disabilitata, questo box stabilisce se ogni messaggio inviato deve essere inserito direttamente nel deposito, o se deve essere messo in un deposito temporaneo in attesa che l'amministratore decida se confermarlo o meno nel deposito vero e proprio. Questo parametro perde di significato qualora l'autenticazione utente sia abilitata.

La sezione Utenti viene utilizzata per definire gli utenti e relative credenziali (password) con cui possono accedere all'uploader. Da notare che il checkbox Conferma automatica ha lo stesso significato del checkbox Conferma ogni messaggio ma si applica ad ogni singolo utente quando l'autenticazione è attiva (e l'altro perde dunque di significato).

Le opzioni "Salva" e "Annulla le modifiche" servono rispettivamente per salvare o leggere da disco le configurazioni, lettura che elimina tutte le modifiche inserite fino a quel momento e non ancora salvate.

Riavvio del configuratore

Il link Riavvia del Configuratore serve a riavviare il configuratore. Questa operazione è necessaria dopo aver cambiato la configurazione dello stesso.

Capitolo 22. Inserimento Spam

Questa sezione viene utilizzata dagli utenti per inviare i campioni di ham e spam. L'amministratore potrà controllare i messaggi inviati e approvare l'entrata di questi ultimi nel deposito, oppure consentire che questo processo avvenga automaticamente.

Se si desiderano maggiori informazioni sulla gestione dei diritti utenti riguardo l'invio dei campioni di ham e spam vedere la sezione chiamata «Utenti dell'inserimento Spam»

La sezione di uploading è suddivisa in due sotto sezioni:

- *Invio tramite file*: permette di inviare un file di testo come campione di ham o spam (utilizzando i rispettivi pulsanti). L'utente dovrà prima salvare su disco in formato testuale il messaggio di posta (si consiglia di salvare anche gli header del messaggio) e poi inserire tale file nella casella File da inviare.

- *Invio testo*: in alternativa è possibile incollare nel box sottostante il testo precedentemente copiato dal client di posta nella clipboard e inviarlo al server senza dover salvare il file temporaneamente su disco.

Una volta arrivato sul server, a seconda delle impostazioni scelte dall'amministratore, il file verrà o trattenuto in un deposito temporaneo in attesta che l'amministratore confermi l'operazione, oppure verrà automaticamente trasferito nel deposito definitivo.

Indipendentemente dalla modalità di invio scelta si consiglia di inserire oltre al testo del messaggio anche gli header al fine di fornire al motore antispam la maggior quantità possibile di informazioni.

Capitolo 23. Quarantena Utente

Questa sezione permette all'utente di accedere ai propri messaggi, bloccati in quanto ritenuti spam/phishing o virati o in violazione di una politica aziendale. Da questa sezione è possibile accedere ai messaggi, prenderne visione, cancellarli ed eventualmente rilasciarli, permettendo così la loro ricezione da parte dell'utente. L'azione di "rilascio" è utilizzabile solo per i messaggi ritenuti spam/phishing, per gli altri casi (virus o in violazione della politica aziendale definita dai filtri) questa operazione non è permessa. Questa limitazione evita che l'utente possa accidentalmente rilasciare un virus o un messaggio bloccato dal sistema di filtraggio, quindi un messaggio che secondo le intenzioni dell'amministratore deve essere bloccato.

La pagina di gestione delle quarantene utente è accessibile solamente mediante il link inviato via mail e non può essere indovinato o dedotto. Ad ogni nuovo report di quarantena, il link precedente viene disabilitato, quindi l'unico link valido è quello relativo all'ultima mail ricevuta.

La schermata mostra in alto l'indirizzo email a cui è relativo il report e la data e l'ora in cui è stato generato. Sotto sono riportate le tabelle a cui è relativo il report.

- Spam: la tabella mostra tutti i messaggi considerati spam/phishing e per questo bloccati.
- Virus: la tabella mostra tutti i messaggi ritenuti virati o in violazione delle norma aziendali.

Le azioni che possono essere applicate su questi messaggi sono : "Rilascia" (solo per lo spam) e "Rimuovi".

Le tabelle mostrano le seguenti informazioni per ciascun messaggio: "Identificativo", "Mittente", "Subject", "Score" e "Data di ricezione". Cliccando sul triangolo a fianco di ciascun titolo è possibile ordinare le mail in funzione delle diverse colonne in modo crescente o descrescente.

Una volta selezionati i messaggi su cui agire, cliccando sui checkbox di ciascun messaggio, è possibile scegliere l'azione di rimozione o rilascio e l'azione sarà relativa ai soli messaggi selezionati. Una volta scelta l'azione è necessario confermare in una seconda schermata la scelta fatta. Per scegliere tutti i messaggi è sufficiente cliccare sul checkbox presente sull'intestazione della tabella.

Quando si rilascia un messaggio, viene data la possibilità di considerare le email come campioni di ham, infatti se si rilascia una email significa che è stata categorizzata in modo errato e per questo si può desiderare di utilizzarla come campione di ham (mail buona) nel database di spam. Per default il flag "Usa come Ham", cioè utilizza il messaggio rilasciato come campione di ham, è attivo.

Appendice A. Legal Notice – Copyright

Questo programma contiene le seguenti librerie e/o programmi

PSF LICENSE AGREEMENT FOR PYTHON 2.2.3

1. This LICENSE AGREEMENT is between the Python Software Foundation
("PSF"), and the Individual or Organization ("Licensee") accessing and
otherwise using Python 2.2.3 software in source or binary form and its

associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty−free, world−wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.2.3 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003 Python Software Foundation; All Rights Reserved" are retained in Python 2.2.3 alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.2.3 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.2.3.

4. PSF is making Python 2.2.3 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.2.3 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.2.3 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.2.3, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python 2.2.3, Licensee agrees to be bound by the terms and conditions of this License Agreement.

SpamBayes

Copyright (C) 2002−2003 Python Software Foundation; All Rights Reserved

The Python Software Foundation (PSF) holds copyright on all material in this project. You may use it under the terms of the PSF license:

PSF LICENSE AGREEMENT FOR THE SPAMBAYES PROJECT
−−

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using the spambayes software ("Software") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty−free, world−wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2002−2003 Python Software Foundation; All Rights Reserved" are retained the Software alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates the Software or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to the Software.

4. PSF is making the Software available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using the Software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

The Python Imaging Library

The Python Imaging Library is

Copyright (c) 1997−2005 by Secret Labs AB
Copyright (c) 1995−2005 by Fredrik Lundh

By obtaining, using, and/or copying this software and/or its
associated documentation, you agree that you have read, understood,
and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its
associated documentation for any purpose and without fee is hereby
granted, provided that the above copyright notice appears in all
copies, and that both that copyright notice and this permission notice
appear in supporting documentation, and that the name of Secret Labs
AB or the author not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior
permission.

SECRET LABS AB AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS. IN NO EVENT SHALL SECRET LABS AB OR THE AUTHOR BE LIABLE FOR
ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modulo DNS (pydns)

This code is covered by the standard Python License.

This code was originally based on the DNS library created
by Guido van Rossum somewhere near the dawn of time.

Since then, as well as myself (Anthony), I have had contributions
by:

Michael Stroeder
Bastian Kleineidam
Timothy J. Miller
Wolfgang Strobl

It's possible there's other people – the old RCS logs for my
code were lost some time ago. The list above is almost certainly
incomplete – let me know if I've forgotten you...

GNU Ocrad

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110−1301 USA
Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If

identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine−readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine−readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as

distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty−free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing

to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER

PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110−1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse−clicks or menu items−−whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Open Directory (DMOZ)

eXtensiveControl® utilizza una parte dei contenuti di Open Directory. I contenuti sono integrati con dati non provenienti dal progetto Open Directory

The Open Directory is a compilation of many different editors' contributions. Netscape Communications Corporation (`Netscape') owns the copyright to the compilation of the different contributions, and makes the Open Directory available to you to use under the following license agreement terms and conditions (`Open Directory License'). For purposes of this Open Directory License, `Open Directory' means only the Open Directory Project currently hosted at http://dmoz.org (or at another site as may be designated by Netscape in the future), and does not include any other versions of directories, even if referred to as an `Open Directory,' that may be hosted by Netscape on other web pages (e.g., Netscape Netcenter).

1. Basic License. Netscape grants you a non−exclusive, royalty−free license to use, reproduce, modify and create derivative works from, and distribute and publish the Open Directory and your derivative works thereof, subject to all of the terms and conditions of this Open Directory License. You may authorize others to exercise the foregoing rights; provided, however, that you must have an agreement with your sublicensees that passes on the requirements and obligations of Sections 2 and 4 below and which must include a limitation of liability provision no less protective of Netscape than Section 6 below.

   Due to the nature of the content of the Open Directory, many third parties' trade names and trademarks will be identified within the content of the Open Directory (e.g., as part of URLs and description of link). Except for the limited license to use the Netscape attribution in Section 2 below, nothing herein shall be deemed to grant you any license to use any Netscape or third party trademark or tradename.
2. Attribution Requirement. As a material condition of this Open Directory License, you must provide the below applicable attribution statements on (1) all copies of the Open Directory, in whole or in part, and derivative works thereof which are either distributed (internally or otherwise) or published (made available on the Internet and/or internally over any internal network/intranet or otherwise), whether distributed or published electronically, on hard copy media or by any other means, and (2) on any program/web page from which you directly link to/access any information contained within the Open Directory, in whole or in part, or any derivative work thereof:

   a. If the Open Directory in whole or in part, or any derivative work thereof, is made available via the Internet or internal network/intranet and/or information contained therein is directly accessed or linked via the Internet or internal network/intranet then you must provide the appropriate Netscape attribution statement as described in the page(s) at the URL(s): http://dmoz.org/become_an_editor.
   b. If the Open Directory in whole or in part, or any derivative work thereof, is made available on any hard copy media (e.g., CD−ROM, diskette), you must place on the packaging a notice providing Netscape attribution as described in the page(s) at the URL(s):

http://dmoz.org/become_an_editor. If there is no `packaging', the previous attribution notice should be placed conspicuously such that it would be reasonably viewed by the recipient of the Open Directory.

c. If you are using or distributing the Open Directory in modified form (i.e., with additions or deletions), you must include a statement indicating you have made modifications to it. Such statement should be placed with the attribution notices required by Sections 2(a) and 2(b) above.

Netscape grants you the non−exclusive, royalty−free license to use the above identified Netscape attribution statements solely for the purpose of the above attribution requirements, and such use must be in accordance with the usage guidelines that may be published by Netscape from time to time as part of the above URLs.

3. Right To Identify Licensee. You agree that Netscape has the right to publicly identify you as a user/licensee of the Open Directory.
4. Errors and Changes. From time to time Netscape may elect to post on the page(s) at the URL http://dmoz.org/become_an_editor certain specific changes to the Open Directory and/or above attribution statements, which changes may be to correct errors and/or remove content alleged to be improperly in the Open Directory. So long as you are exercising the license to Open Directory hereunder, you agree to use commercially reasonable efforts to check the page(s) at the URL http://dmoz.org/become_an_editor from time to time, and to use commercially reasonable efforts to make the changes/corrections/deletion of content from the Open Directory and/or attribution statements as may be indicated at such URL. Any changes to the Open Directory content posted at the page(s) at the URL http://dmoz.org/become_an_editor are part of Open Directory.
5. No Warranty/Use At Your Risk. THE OPEN DIRECTORY AND ANY NETSCAPE TRADEMARKS AND LOGOS CONTAINED WITH THE REQUIRED ATTRIBUTION STATEMENTS ARE MADE AVAILABLE UNDER THIS OPEN DIRECTORY LICENSE AT NO CHARGE. ACCORDINGLY, THE OPEN DIRECTORY AND THE NETSCAPE TRADEMARKS AND LOGOS ARE PROVIDED `AS IS,' WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION THE WARRANTIES THAT THEY ARE MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON−INFRINGING. YOU ARE SOLELY RESPONSIBLE FOR YOUR USE, DISTRIBUTION, MODIFICATION, REPRODUCTION AND PUBLICATION OF THE OPEN DIRECTORY AND ANY DERIVATIVE WORKS THEREOF BY YOU AND ANY OF YOUR SUBLICENSEES (COLLECTIVELY, `YOUR OPEN DIRECTORY USE'). THE ENTIRE RISK AS TO YOUR OPEN DIRECTORY USE IS BORNE BY YOU. YOU AGREE TO INDEMNIFY AND HOLD NETSCAPE, ITS SUBSIDIARIES AND AFFILIATES HARMLESS FROM ANY CLAIMS ARISING FROM OR RELATING TO YOUR OPEN DIRECTORY USE.
6. Limitation of Liability. IN NO EVENT SHALL NETSCAPE, ITS SUBSIDIARIES OR AFFILIATES, OR THE OPEN DIRECTORY CONTRIBUTING EDITORS, BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF ADVISED OF THE POSSIBILITY THEREOF, AND REGARDLESS OF WHETHER ANY CLAIM IS BASED UPON ANY CONTRACT, TORT OR OTHER LEGAL OR EQUITABLE THEORY, RELATING OR ARISING FROM THE OPEN DIRECTORY, YOUR OPEN DIRECTORY USE OR THIS OPEN DIRECTORY LICENSE AGREEMENT.
7. California Law. This Open Directory License will be governed by the laws of the State of California, excluding its conflict of laws provisions.

OpenSSL License

/* ==

* Copyright (c) 1998−2000 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

```
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non−commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :−).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
* PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
```

* [including the GNU Public Licence.]
*/

GD lib

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant P41−RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README−JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user−accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user−accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank

David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant P41−RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README−JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user−accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user−accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

ZLIB

PNG

```
*
*    There is no warranty against interference with your enjoyment of the
*    library or against infringement.  There is no warranty that our
*    efforts or the library will fulfill any of your particular purposes
*    or needs.  This library is provided with all faults, and the entire
*    risk of satisfactory quality, performance, accuracy, and effort is with
*    the user.
*
* libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are
* Copyright (c) 1998, 1999, 2000 Glenn Randers−Pehrson
* Distributed according to the same disclaimer and license as libpng−0.96,
* with the following individuals added to the list of Contributing Authors:
*
*    Tom Lane
*    Glenn Randers−Pehrson
*    Willem van Schaik
*
* libpng versions 0.89, June 1996, through 0.96, May 1997, are
* Copyright (c) 1996, 1997 Andreas Dilger
* Distributed according to the same disclaimer and license as libpng−0.88,
* with the following individuals added to the list of Contributing Authors:
*
*    John Bowler
*    Kevin Bracey
*    Sam Bushell
*    Magnus Holmgren
*    Greg Roelofs
*    Tom Tanner
*
* libpng versions 0.5, May 1995, through 0.88, January 1996, are
* Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.
*
* For the purposes of this copyright and license, "Contributing Authors"
* is defined as the following set of individuals:
*
*    Andreas Dilger
*    Dave Martindale
*    Guy Eric Schalnat
*    Paul Schmidt
*    Tim Wegner
*
* The PNG Reference Library is supplied "AS IS".  The Contributing Authors
* and Group 42, Inc. disclaim all warranties, expressed or implied,
* including, without limitation, the warranties of merchantability and of
* fitness for any purpose.  The Contributing Authors and Group 42, Inc.
* assume no liability for direct, indirect, incidental, special, exemplary,
* or consequential damages, which may result from the use of the PNG
* Reference Library, even if advised of the possibility of such damage.
*
* Permission is hereby granted to use, copy, modify, and distribute this
* source code, or portions hereof, for any purpose, without fee, subject
* to the following restrictions:
*
* 1. The origin of this source code must not be misrepresented.
```

```
*
* 2. Altered versions must be plainly marked as such and
* must not be misrepresented as being the original source.
*
* 3. This Copyright notice may not be removed or altered from
*    any source or altered source distribution.
*
* The Contributing Authors and Group 42, Inc. specifically permit, without
* fee, and encourage the use of this source code as a component to
* supporting the PNG file format in commercial products.  If you use this
* source code in a product, acknowledgment is not required but would be
* appreciated.
*/
```

JPEG

This software is copyright (C) 1991−1998, Thomas G. Lane.
All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this
software (or portions thereof) for any purpose, without fee, subject to these
conditions:
(1) If any part of the source code for this software is distributed, then this
README file must be included, with this copyright and no−warranty notice
unaltered; and any additions, deletions, or changes to the original files
must be clearly indicated in accompanying documentation.
(2) If only executable code is distributed, then the accompanying
documentation must state that "this software is based in part on the work of
the Independent JPEG Group".
(3) Permission for use of this software is granted only if the user accepts
full responsibility for any undesirable consequences; the authors accept
NO LIABILITY for damages of any kind.

PCRE

PCRE LICENCE
−−−−−−−−−−−−

PCRE is a library of functions to support regular expressions whose syntax
and semantics are as close as possible to those of the Perl 5 language.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,
Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997−2001 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any

computer system, and to redistribute it freely, subject to the following
restrictions:

1. This software is distributed in the hope that it will be useful,
   but WITHOUT ANY WARRANTY; without even the implied warranty of
   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by
   explicit claim or by omission. In practice, this means that if you use
   PCRE in software which you distribute to others, commercially or
   otherwise, you must put a sentence like this

     Regular expression support is provided by the PCRE library package,
     which is open source software, written by Philip Hazel, and copyright
     by the University of Cambridge, England.

   somewhere reasonably visible in your documentation and in any relevant
   files or online help data or similar. A reference to the ftp site for
   the source, that is, to

     ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

   should also be given in the documentation.

3. Altered versions must be plainly marked as such, and must not be
   misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU
   General Purpose Licence (GPL), or Lesser General Purpose Licence (LGPL),
   then the terms of that licence shall supersede any condition above with
   which it is incompatible.

The documentation for PCRE, supplied in the "doc" directory, is distributed
under the same terms as the software itself.

End

Reportlab PDF Library

```
#############################################################################
#
#     Copyright (c) 2000−2004, ReportLab Inc.
#     All rights reserved.
#
#     Redistribution and use in source and binary forms, with or without modification,
#     are permitted provided that the following conditions are met:
#
#           *      Redistributions of source code must retain the above copyright notice,
#                  this list of conditions and the following disclaimer.
#           *      Redistributions in binary form must reproduce the above copyright notice,
#                  this list of conditions and the following disclaimer in the documentation
#                  and/or other materials provided with the distribution.
```

```
#           *  Neither the name of the company nor the names of its contributors may be
#              used to endorse or promote products derived from this software without
#              specific prior written permission.
#
#     THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
#     ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
#     WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAI
#     IN NO EVENT SHALL THE OFFICERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT
#     INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LI
#     TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
#     OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETH
#     IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISINC
#     IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
#     SUCH DAMAGE.
#
##############################################################################
```

File

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.
Software written by Ian F. Darwin and others;
maintained 1994–2003 Christos Zoulas.

This software is not subject to any export provision of the United States
Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice immediately at the beginning of the file, without modification,
   this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
   This product includes software developed by Ian F. Darwin and others.
4. The name of the author may not be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

PLY

PLY (Python Lex−Yacc) Version 1.5 (June 1, 2004)

David M. Beazley
Department of Computer Science
University of Chicago
Chicago, IL 60637
beazley@cs.uchicago.edu

Introduction
============

PLY is a 100% Python implementation of the common parsing tools lex
and yacc. Although several other parsing tools are available for
Python, there are several reasons why you might want to consider PLY:

- The tools are very closely modeled after traditional lex/yacc.
  If you know how to use these tools in C, you will find PLY
  to be similar.

- PLY provides *very* extensive error reporting and diagnostic
  information to assist in parser construction. The original
  implementation was developed for instructional purposes. As
  a result, the system tries to identify the most common types
  of errors made by novice users.

- PLY provides full support for empty productions, error recovery,
  precedence specifiers, and moderately ambiguous grammars.

- Parsing is based on LR−parsing which is fast, memory efficient,
  better suited to large grammars, and which has a number of nice

properties when dealing with syntax errors and other parsing problems.
Currently, PLY builds its parsing tables using the SLR algorithm which
is slightly weaker than LALR(1) used in traditional yacc.

- Like John Aycock's excellent SPARK toolkit, PLY uses Python
reflection to build lexers and parsers. This greatly simplifies
the task of parser construction since it reduces the number of files
and eliminates the need to run a separate lex/yacc tool before
running your program.

- PLY can be used to build parsers for "real" programming languages.
Although it is not ultra−fast due to its Python implementation,
PLY can be used to parse grammars consisting of several hundred
rules (as might be found for a language like C). The lexer and LR
parser are also reasonably efficient when parsing typically
sized programs.

The original version of PLY was developed for an Introduction to
Compilers course where students used it to build a compiler for a
simple Pascal−like language. Their compiler had to include lexical
analysis, parsing, type checking, type inference, and generation of
assembly code for the SPARC processor. Because of this, the current
implementation has been extensively tested and debugged. In addition,
most of the API and error checking steps have been adapted to address
common usability problems.

How to Use
==========

PLY consists of two files : lex.py and yacc.py. To use the system,
simply copy these files to your project and import them like standard
Python modules.

The file doc/ply.html contains complete documentation on how to use
the system.

The example directory contains several different examples including a
PLY specification for ANSI C as given in K&R 2nd Ed. Note: To use
the examples, you will need to copy the lex.py and yacc.py files to
the example directory.

A simple example is found at the end of this document

Requirements
============
PLY requires the use of Python 2.0 or greater. It should work on
just about any platform.

Resources
=========

More information about PLY can be obtained on the PLY webpage at:

http://systems.cs.uchicago.edu/ply

For a detailed overview of parsing theory, consult the excellent
book "Compilers : Principles, Techniques, and Tools" by Aho, Sethi, and
Ullman. The topics found in "Lex & Yacc" by Levine, Mason, and Brown
may also be useful.

Acknowledgments
==========

A special thanks is in order for all of the students in CS326 who
suffered through about 25 different versions of these tools :-).

The CHANGES file acknowledges those who have contributed patches.

Example
=======

Here is a simple example showing a PLY implementation of a calculator with variables.

```
# -----------------------------------------------------------------------------
# calc.py
#
# A simple calculator with variables.
# -----------------------------------------------------------------------------

tokens = (
    'NAME','NUMBER',
    'PLUS','MINUS','TIMES','DIVIDE','EQUALS',
    'LPAREN','RPAREN',
    )

# Tokens

t_PLUS    = r'\+'
t_MINUS   = r'-'
t_TIMES   = r'\*'
t_DIVIDE  = r'/'
t_EQUALS  = r'='
t_LPAREN  = r'\('
t_RPAREN  = r'\)'
t_NAME    = r'[a-zA-Z_][a-zA-Z0-9_]*'

def t_NUMBER(t):
    r'\d+'
    try:
        t.value = int(t.value)
    except ValueError:
        print "Integer value too large", t.value
        t.value = 0
    return t

# Ignored characters
t_ignore = " \t"
```

```
def t_newline(t):
    r'\n+'
    t.lineno += t.value.count("\n")

def t_error(t):
    print "Illegal character '%s'" % t.value[0]
    t.skip(1)

# Build the lexer
import lex
lex.lex()

# Precedence rules for the arithmetic operators
precedence = (
    ('left','PLUS','MINUS'),
    ('left','TIMES','DIVIDE'),
    ('right','UMINUS'),
    )

# dictionary of names (for storing variables)
names = { }

def p_statement_assign(p):
    'statement : NAME EQUALS expression'
    names[p[1]] = p[3]

def p_statement_expr(p):
    'statement : expression'
    print p[1]

def p_expression_binop(p):
    '''expression : expression PLUS expression
                  | expression MINUS expression
                  | expression TIMES expression
                  | expression DIVIDE expression'''
    if p[2] == '+'  : p[0] = p[1] + p[3]
    elif p[2] == '-': p[0] = p[1] - p[3]
    elif p[2] == '*': p[0] = p[1] * p[3]
    elif p[2] == '/': p[0] = p[1] / p[3]

def p_expression_uminus(p):
    'expression : MINUS expression %prec UMINUS'
    p[0] = -p[2]

def p_expression_group(p):
    'expression : LPAREN expression RPAREN'
    p[0] = p[2]

def p_expression_number(p):
    'expression : NUMBER'
    p[0] = p[1]

def p_expression_name(p):
    'expression : NAME'
```

```
    try:
        p[0] = names[p[1]]
    except LookupError:
        print "Undefined name '%s'" % p[1]
        p[0] = 0

def p_error(p):
    print "Syntax error at '%s'" % p.value

import yacc
yacc.yacc()

while 1:
    try:
        s = raw_input('calc > ')
    except EOFError:
        break
    yacc.parse(s)
```

c–ares

```
/* Copyright 1998 by the Massachusetts Institute of Technology.
 *
 * Permission to use, copy, modify, and distribute this
 * software and its documentation for any purpose and without
 * fee is hereby granted, provided that the above copyright
 * notice appear in all copies and that both that copyright
 * notice and this permission notice appear in supporting
 * documentation, and that the name of M.I.T. not be used in
 * advertising or publicity pertaining to distribution of the
 * software without specific, written prior permission.
 * M.I.T. makes no representations about the suitability of
 * this software for any purpose.  It is provided "as is"
 * without express or implied warranty.
 */
```

Modulo Socket

```
    Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
```

Modulo fpectl (Floating point exception control)

\ endorsement purposes. /
 ——

MD5 message digest algorithm

Moduli asynchat e asyncore (Asynchronous socket services)

Modulo Cookie

Moduli profile e pstats

CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modulo trace

portions copyright 2001, Autonomous Zones Industries, Inc., all rights...
err... reserved and offered to the public under the terms of the
Python 2.2 license.
Author: Zooko O'Whielacronx
http://zooko.com/
mailto:zooko@zooko.com

Copyright 2000, Mojam Media, Inc., all rights reserved.
Author: Skip Montanaro

Copyright 1999, Bioreason, Inc., all rights reserved.
Author: Andrew Dalke

Copyright 1995−1997, Automatrix, Inc., all rights reserved.
Author: Skip Montanaro

Copyright 1991−1995, Stichting Mathematisch Centrum, all rights reserved.

Permission to use, copy, modify, and distribute this Python software and
its associated documentation for any purpose without fee is hereby
granted, provided that the above copyright notice appears in all copies,
and that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of neither Automatrix,
Bioreason or Mojam Media be used in advertising or publicity pertaining to
distribution of the software without specific, written prior permission

UUencode and UUdecode functions

Copyright 1994 by Lance Ellinghouse
Cathedral City, California Republic, United States of America.
All Rights Reserved
Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Lance Ellinghouse
not be used in advertising or publicity pertaining to distribution
of the software without specific, written prior permission.
LANCE ELLINGHOUSE DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL LANCE ELLINGHOUSE CENTRUM BE LIABLE
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT

OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modified by Jack Jansen, CWI, July 1995:
– Use binascii module to do the actual line–by–line conversion
  between ascii and binary. This results in a 1000–fold speedup. The C
  version is still 5 times faster, though.
– Arguments more compliant with python standard

xmlrpclib

The XML–RPC client interface is