

NETASQ UTM Versione 8.0.2

Elevata performance a protezione del tuo futuro!

Punti salienti

- Routing basato sulle policy
- Proxy FTP e HTTP
- Prevenzione delle intrusioni day zero per il VoIP
- Monitoraggio applicativo

Aggiornamenti

Versione minima richiesta: 7.0.0

Livello delle modifiche

Versione minima richiesta per l'alta disponibilità (HA): 7.0.0

Compatibilità con la versione 8.0.0

F25*	U30
F50*	U70
F60	U120
F200	U250
F500	U450
F800	U1100
F1000	U1500
F1200	U6000
F2000 – F2500	
F5000 – F5500	

*: con alcune restrizioni (vedi colonna a lato)

Politiche di filtro	Minore
SSL VPN	Maggiore
Administration Suite	Minore
ASQ	Minore
Proxy	Maggiore
Alta disponibilità (HA)	Nessuna
Sistema operativo	Critica
NAT	Nessuna

Restrizioni alla compatibilità

Il modulo antivirus non sarà più funzionante sui prodotti F25/B, F25/C e F50/C.

Durante la procedura di aggiornamento, il modulo verrà disabilitato ed il database dell'antivirus cancellato.

Versione 8.0.2

Nuove funzioni: minore

Correzione errori: maggiore

Correzione vulnerabilità: maggiore

Contenuti

[Funzioni 8.0.0](#)

[Vulnerabilità corrette 8.0.0](#)

[Bug fixes 8.0.0](#)

[Funzioni 8.0.1](#)

[Vulnerabilità corrette 8.0.1](#)

[Bug fixes 8.0.1](#)

[Funzioni 8.0.2](#)

[Vulnerabilità corrette 8.0.2](#)

[Bug fixes 8.0.2](#)

[Problemi noti 8.0.0.2](#)

[Problemi noti 8.0.2](#)

Funzioni della versione 8.0.0

Routing basato sulle policy

Integrazione nel motore ASQ

La nuova versione del motore ASQ consente di gestire il routing basato sulle policy all'interno delle policy di filtro, permettendo in tal modo di beneficiare della flessibilità derivante dalle regole di filtro. Ora è possibile indicare nell'apposita nuova colonna "Route" uno specifico router per una data regola di filtro, indirizzando quindi il traffico corrispondente a tale regola al router selezionato. Il routing basato sulle policy può essere impiegato per qualsiasi regola di filtro impostata su "Pass".

Nota: per garantire il corretto funzionamento del routing basato sulle policy è necessario impostare un percorso standard nel menù "route".

Supporto IPSec

È stato modificato il metodo di gestione dei pacchetti ESP. Ciò consente di impostare il routing basato sulle policy anche sul traffico IPSec.

Proxy FTP

Analisi protocollare

Questo proxy controlla i comandi FTP ed effettua la scansione antivirus sui contenuti trasportati attraverso questo protocollo: il sistema controlla solo il trasferimento di file (upload e download). Dato che è il motore ASQ a fornire la protezione contro le intrusioni (analisi protocollare), il proxy FTP analizza in modo più dettagliato numero e natura degli argomenti della riga di comando attraverso tre livelli di verifica:

- Bloccando senza riserve il comando
- Controllando la validità del comando
- Accettando senza riserve il comando

L'analisi protocollare e la scansione antivirus permettono inoltre di proteggere i server FTP con un proprio indirizzo IP pubblico.

Poiché la scansione antivirus viene effettuata su tutto il file scaricato, il proxy FTP ne dilata il trasferimento per preservare la validità della connessione con il client (timeout). Per ragioni di sicurezza (ossia per evitare il trasferimento di virus in diversi frammenti), il proxy FTP non permette trasferimenti parziali dei file (sistema usato da meccanismi che continuano il trasferimento dopo una eventuale disconnessione). Allo stesso modo, per diminuire il rischio di attacchi "bounce", il trasferimento FXP non è permesso.

Le informazioni raccolte nei log sulle connessioni FTP sono salvate in un file specifico. Oltre ai campi standard (Id, fw, starttime, src, srcport, etc), le informazioni raccolte nei log presenteranno i seguenti campi aggiuntivi:

- Op: comando FTP espletato
- User: utente autorizzato
- GroupId: ID di session impiegato per collegare i comandi al trasferimento di dati.

Gestione dei comandi FTP

Poiché i server FTP non supportano tutti i comandi del protocollo, esiste un comando protocollare (FEAT) che permette di visualizzare la lista dei comandi supportati. Il proxy FTP agisce tra i server filtrando le funzioni annunciate dai server in base alle autorizzazioni impostate dall'amministratore. Il proxy FTP può essere configurato per aggiungere comandi FTP personalizzati che non sono stati definiti dagli RFC.

Per semplificare la scelta dei comandi da bloccare, il proxy FTP impiega un valore che permette di raggruppare insieme tutti i comandi relativi al trasferimento di file. Il valore "UPLOAD" raggruppa i comandi FTP STOR, STOU, APPE, ALLO, RNFR, RNFO, DELE, RMD e MKD.

Infine, il proxy FTP dei dispositivi NETASQ supporta la messa in coda di più comandi FTP rispedendoli al server.

Modalità di trasferimento

Il protocollo FTP necessita l'impiego di due connessioni – una per i comandi inizializzati dall'utente ed una per i dati inizializzati secondo il metodo di trasferimento selezionato. Sebbene l'implementazione del proxy FTP sia trasparente per l'utente finale, il proxy intercetta eventuali comandi FTP nei parametri di connessione dell'utente ed inizializza la connessione al server.

Il proxy FTP permette inoltre di definire con precisione le modalità di trasferimento (all/ active/ passive). Nella configurazione standard la modalità impostata è "all", parametro modificabile a piacimento dall'utente.

Definendo una particolare modalità di trasferimento (attiva o passiva) per le connessioni con il server, questa verrà impiegata per i collegamenti tra il dispositivo NETASQ ed il server FTP, indipendentemente dalla modalità selezionata dal client. Tuttavia, la configurazione di una modalità specifica per le connessioni tra l'appliance NETASQ ed il client FTP darà luogo ad una limitazione delle modalità di trasmissione selezionabili dal client.

NETASQ UNIFIED MANAGER

Il NETASQ UNIFIED MANAGER offre numerose funzioni per la gestione dei parametri del proxy FTP. In tal modo, l'amministratore può:

- Attivare l'antivirus e definire il comportamento dell'appliance NETASQ (blocca/accetta su rilevamento e blocca/accetta in caso di fallimento dell'analisi)
- Configurare il comportamento dell'appliance secondo i comandi FTP analizzati
- Definire un elenco di server autorizzati
- Definire un elenco dei server su cui non vengono applicati l'antivirus e le funzioni di controllo dei comandi
- Configurare le modalità di trasferimento di client e server

Proxy HTTP esplicito

Funzionamento

Il proxy HTTP esplicito estende le caratteristiche del proxy HTTP esistente. Offre altresì le stesse funzioni di filtraggio URL e antivirus attraverso l'interfaccia grafica che rimane la stessa. Per evitare di gravare sulle performance, si consiglia di non abilitare i servizi ICAP su un proxy HTTP esplicito.

L'accesso sicuro ai server web (protocollo HTTPS) attraverso il proxy HTTP esplicito viene effettuato tramite il metodo "Connect". Per ragioni di sicurezza inerenti all'impiego di tale metodologia, il protocollo "FTP su HTTP" non può essere impiegato attraverso il proxy HTTP esplicito.

Rilevamento automatico del proxy

L'impostazione di un proxy HTTP esplicito comprende una connessione diretta del browser all'appliance NETASQ. La configurazione del browser sui client viene semplificata con l'implementazione del protocollo WPAD sull'appliance NETASQ. Questo protocollo si traduce nel trasferimento di un file che può essere usato sia dal DHCP sia dal portale dell'appliance, attraverso cui si possono impostare configurazioni limitate all'impiego per interfaccia. Questo file assicura inoltre che la connessione al portale di autenticazione dell'appliance non sia gestita dal proxy HTTP esplicito.

Autenticazioni multiple dallo stesso indirizzo IP

L'abilitazione del proxy http esplicito consente a più utenti di autenticarsi da un unico indirizzo IP (Citrix o ambiente TSE virtuale).

Risk management: NETASQ SEISMO

Monitoraggio delle applicazioni

NETASQ SEISMO è stato aggiornato e permette ora di rilevare le applicazioni implementate nell'azienda suddividendole in due categorie:

- **Prodotti**, applicativi client installati su una postazione di lavoro (es. FireFox 1.5)
- **Servizi**, applicativi server su una porta specifica (es. OpenSSH 3.5).

Impiegando i dati rilevati dal motore ASQ, NETASQ SEISMO genera informazioni sulle applicazioni identificate. L'aggiunta di tale funzione consente di raggruppare le applicazioni in famiglie. Comparando questa informazione con il database delle vulnerabilità, NETASQ SEISMO indicherà le vulnerabilità collegate a queste applicazioni.

La rilevazione delle applicazioni è inoltre raccolta in log che presenteranno due nuovi campi: "product" e "service".

NETASQ REAL-TIME MONITOR

Finestra SEISMO

Alla finestra SEISMO dell'applicazione NETASQ REAL-TIME MONITOR è stata aggiunto il pannello "Application(s)". Come per gli altri pannelli, sono disponibili opzioni quali filtering, visualizzazione opzionale delle colonne, ridimensionamento in base al contenuto e copia dei dati al clipboard. Questa schermata offre informazioni sulle applicazioni rilevate presentandole nelle seguenti colonne:

- **Name:** indica il nome del software senza specificare la versione (ad esclusione dei sistemi operativi)
- **Family:** mostra la famiglia del software dell'applicazione (esempio: "web client")
- **Application type:** permette di identificare il tipo di software (client: il software non offre servizi – server: il software offre servizi – sistema operativo)
- **Instance:** indica il numero di software in esecuzione.

Quando si seleziona una particolare applicazione, il NETASQ REAL-TIME MONITOR mostra, in fondo al pannello "Application(s)", un elenco dettagliato con le seguenti informazioni:

- **Name column:** mostra il nome dell'host
- **Address column:** mostra l'indirizzo IP dell'host
- **Application column:** mostra il nome e, se disponibile, la versione del software
- **Application type column:** specifica il tipo di software (client: il software non offre servizi – server: il software offre servizi – sistema operativo)
- **Operating system column:** mostra il sistema operativo della postazione di lavoro
- **Port column:** mostra la porta utilizzata dal software (se in uso)
- **Internet protocol column:** mostra il protocollo internet del software (se in uso)

Inoltre, se si seleziona un particolare host da questa presentazione dettagliata (finestra SEISMO, "Application(s)"), il menu contestuale mostrerà l'host selezionato (schermata "host").

Il pannello "Information" si chiama ora "Event(s)". La panoramica dettagliata offerta dal pannello "Vulnerabilities" e "Event(s)" è stata modificata per mostrare più chiaramente le informazioni relative alle applicazioni. La colonna "Service" si chiama ora "Software" e mostra la versione del software, se disponibile. È stata aggiunta la colonna "Event(s)", in cui viene indicato il tipo di applicazione (Client / Server / Sistema operativo).

Finestra host

Mettendo in pratica il perfezionamento di NETASQ SEISMO inerente alla rilevazione delle applicazioni, la finestra "Host" è stata modificata come segue:

- Aggiunta della colonna "Applications" che mostra il numero di applicazioni software (client / server) presenti
- Sostituzione del menu "Service" con il menu "Applications"

Il pannello "Applications" presente nella finestra "host", nell'area che mostra informazioni dettagliate, presenta le seguenti colonne:

- **Version:** mostra nome e versione del software
- **Vulnerability:** mostra il numero di vulnerabilità individuate sul software
- **Family:** mostra la famiglia del software
- **Type:** permette di identificare il tipo di software (client: il software non offre servizi – server: il software offre servizi – sistema operativo)
- **Port:** mostra la porta utilizzata dal software (se in uso)
- **Internet protocol:** mostra il protocollo internet del software (se in uso)

Quando si seleziona una particolare applicazione nel pannello "Applications", il NETASQ REAL-TIME MONITOR renderà operative le funzioni che permettono:

- La visualizzazione di host che hanno lo stesso software installato
- La visualizzazione delle vulnerabilità del software
- La modifica del software dell'host (solo per i server)

Il pannello "Vulnerability" nella sezione delle informazioni dettagliate della finestra "host" è stata modificata e ora presenta le seguenti colonne:

- **Application name:** mostra il nome e, se disponibile, la versione del software
- **Type:** specifica il tipo di software (client: il software non offre servizi – server: il software offre servizi – sistema operativo)

Applicazione delle firme contestuali

Per ottenere il massimo dal motore ASQ, le firme inerenti agli applicativi sono state integrate nelle firme contestuali del motore ASQ. Oltre al miglioramento della performance, questo permette di mutuare la supervisione tra attacchi e vulnerabilità. Le firme inerenti agli applicativi vengono automaticamente aggiornate dal modulo ActiveUpdate. Il formato dei dati di SEISMO è stato aggiornato e di conseguenza i database della versione 7 sono incompatibili con quelli della versione 8.

Motore ASQ

VoIP: plugin di analisi e prevenzione SIP

SIP è un protocollo che permette l'instaurarsi di una connessione VoIP per le comunicazioni client-server (telefono, IPBX, server vocale, proxy SIP) o per conferenze telefoniche. Una volta che la comunicazione è stata stabilita, nel contesto di uno scambio tra postazioni di lavoro, si impiegano due canali per il trasporto dei dati (da A a B e da B ad A). Il plugin SIP sul motore ASQ creerà due connessioni per ogni canale: una per il trasferimento dei dati RTP e l'altra per le informazioni RTCP.

Per proteggere contro attacchi sul protocollo SIP, il plugin SIP definisce tre contesti di applicazione: SIP.Request, SIP.Header e SIP.SDP.

Il NETASQ UNIFIED MANAGER permette di configurare numerosi parametri sul plugin SIP, ad esempio l'attivazione o disattivazione dell'impiego del protocollo SIP via UDP e/o TCP. Per quanto riguarda le funzioni SIP, quelle supportate di default possono essere bloccate (operazioni SIP standard e operazioni derivanti dagli interni) oppure si possono autorizzare nuove funzioni (implementate ad esempio in specifici telefoni o derivanti da nuovi interni). L'applicazione permette inoltre di configurare parametri avanzati quali le dimensioni del buffer o la durata massima di una sessione.

L'implementazione del protocollo SIP comprende altresì l'impostazione di nuovi allarmi e la creazione di nuovi campi per le informazioni raccolte nel log. Il plugin SIP viene abilitato di default durante l'aggiornamento del software delle appliance NETASQ.

VoIP: plugin di analisi e prevenzione MGCP

Il plugin MGCP è stato aggiornato. Beneficia ora dei miglioramenti apportati al trattamento del protocollo SDP. Sono inoltre disponibili i seguenti allarmi:

- Overflow in MGCP
- Possibile malware nei parametri MGCP
- Parametro proibito nel MGCP
- Campo obbligatorio SPD mancante nel MGCP
- Superamento del limite di operazioni consentite con MGCP

Inoltre, il modulo delle firme contestuali è stato riorganizzato in tre sottomoduli: MGCP.Command, MGCP.Param e MGCP.SDP.

Applicazione di rilevazione delle intrusioni

È ora possibile impostare il motore di prevenzione delle intrusioni ASQ in modalità "rilevazione delle intrusioni". In questo modo, anziché bloccare il traffico sospetto, il sistema si limiterà solo a lanciare un allarme. Questa modalità è configurabile nel NETASQ UNIFIED MANAGER e comprende allarmi non configurabili nella precedente versione quando il sistema veniva impostato su "Pass".

Il NETASQ UNIFIED MANAGER permette di passare dalla modalità di prevenzione alla modalità di rilevazione delle intrusioni indicando l'azione "Pass". Poiché questa modifica influisce sul livello di sicurezza, la finestra di configurazione di ASQ contiene ora una nuova colonna – "Sensitive" – che mostra un'icona simboleggiante gli avvisi giudicati critici. Allo stesso modo, l'applicazione NETASQ REAL-TIME MONITOR presenta questa colonna nella schermata "Alarms".

Inoltre, dato che il motore ASQ opera conducendo analisi in successione, ognuna delle quali facente affidamento sui risultati dell'analisi precedente, disabilitare uno di questi livelli di trattamento potrebbe intaccare i risultati del trattamento seguente. Di conseguenza, non appena il motore ASQ identifica un allarme "Sensitive" impostato su "Pass", l'analisi applicativa ad esso associata viene disabilitata riducendo l'analisi ai livelli inferiori (IP, ICMP, TCP, o UDP).

Plugin HTTP

Il plugin HTTP è stato modificato per migliorare l'analisi del protocollo HTTP, che offre ora i seguenti allarmi:

- **"Site with open redirect"**: abilita l'identificazione dei rimbalzi dei siti web dopo un reindirizzamento (allarme impostato su "Pass" per il traffico in uscita – profilo 01).
- **"304 response with message body"**: viene lanciato quando la risposta di un sito web indica che sebbene la pagina richiesta non sia stata modificata dall'ultima richiesta (codice 304) trasmette comunque i dati. La configurazione standard di questo allarme dipende dal profilo:
 - Per il traffico in entrata (profilo 00) l'allarme è impostato su "Block"
 - Per il traffico in uscita (profilo 01) l'allarme è impostato su "Pass"
- **"Additional data at end of reply"**: consente di identificare risposte dei siti web contenenti una quantità di dati che supera quella impostata nel campo "Content-Length".

Nota: Impostare su "Pass" allarmi associati all'identificazione di evasioni di dati attraverso la cifratura Unicode (%u) potrebbe favorire attacchi camuffati.

Plugin DNS

Sono stati aggiunti due nuovi allarmi DNS per completare e specificare le analisi esistenti:

- **"Contradictory "DNS query" field"**: questo allarme identifica le risposte DNS i cui ID corrispondono a query DNS ancora in corso ma il cui campo "query" presenta un valore differente dal campo presente nella query.
- **"Targeted DNS spoofing"**: specifica l'allarme già esistente "DNS id spoofing" (dns: 38) e viene lanciato quando una risposta DNS collegata ad una query conosciuta contiene un ID non valido.

Plugin SSL

Il plugin SSL supporta ora i protocolli TLS 1.1 e TLS 1.2.

IPSec

Ottimizzazione della fase 2 di ricerca delle policy (SPD)

L'algoritmo di ricerca sulle policy di sicurezza IPSec (SPD) è stato migliorato con l'implementazione di un elemento di memoria che agisce come indice dinamico. In un'architettura che contiene un elevato numero di tunnel VPN, questa funzione ottimizza i tempi di ricerca delle policy di cifratura da applicare.

Per preservare l'integrità delle architetture esistenti, questa funzione non viene abilitata durante l'aggiornamento. La funzione è attivabile modificando il file di configurazione dello slot VPN (vedi esempio):

```
[Global]
Tunnels=Tunnel_1
SPDCACHE=16384
```

Policy di sicurezza "No encryption"

Le policy di sicurezza VPN sono applicata ad ogni singolo pacchetto. I pacchetti non criptati vengono quindi confrontati con tutte le policy disponibili prima di essere trattati. Nel caso in cui vi siano più tunnel, questa valutazione potrebbe rallentare il traffico non criptato. Al fine di assicurare un trattamento più rapido, è ora possibile inserire la policy di sicurezza "No encryption" tra le policy VPN.

Nota: l'implementazione di questa policy richiede la disattivazione e riattivazione del corrispondente slot VPN.

Qualità del servizio (QoS)

A fronte dell'implementazione del routing basato sulle policy nel motore ASQ, è possibile gestire la qualità del servizio (QoS) sui protocolli ESP e GRE. Poiché le policy di filtro possono essere collegate a questi protocolli, è possibile associare loro una qualità del servizio per priorità o per classe di applicazione.

Scambio di chiavi

Il modulo IPsec VPN offre tre nuovi gruppi di negoziazione Diffie-Hellman:

- Il gruppo 14 usa una chiave lunga 2048 bit
- Il gruppo 15 usa una chiave lunga 3072 bit
- Il gruppo 16 usa una chiave lunga 4096 bit

Antivirus – Caricamento dinamico del database Kaspersky

Questa opzione permette di installare il database dell'antivirus Kaspersky appena scaricato senza riavviare il servizio. In questo modo, il database dell'antivirus viene aggiornato senza interruzioni nel servizio. Questa opzione è attivata di default e può essere configurata tramite la console.

Nota: Questa funzione è disponibile solo nei seguenti modelli:

- Serie F: F500, F800, F1000, F1200, F2000, F2500, F5000 e F5500
- Serie U: U120, U250, U450, U1100, U1500 e U6000

Reti: capacità VLAN e PPTP

I miglioramenti apportati dai prodotti NETASQ alla gestione della rete riguardano anche i client VLAN e PPTP. I procedimenti, configurabili tramite due diversi pannelli del NETASQ UNIFIED MANAGER, sono identici.

Il principio di base è di consentire la configurazione del massimo numero di interfacce (VLAN or PPTP) entro i limiti stabiliti dal prodotto. Se non viene raggiunto il numero massimo di interfacce configurate, l'amministratore può creare tante VLAN quante ne desidera senza riavviare il sistema. Se si supera il limite, l'appliance ridistribuirà un blocco di 8 VLAN, avvisando l'amministratore che è necessario fare un reboot del dispositivo per rendere operativi i cambiamenti. Il valore del numero massimo riallocabile dai prodotti NETASQ può essere modificato prima del reboot.

Nota: Il numero totale di interfacce configurate può influenzare la performance generale del prodotto: è quindi consigliabile dichiarare solo il numero necessario.

NETASQ UNIFIED MANAGER

Ricerca dei certificati

Il NETASQ UNIFIED MANAGER offre una nuova utility di ricerca: nella finestra "Certificate" è possibile cercare qualsiasi oggetto che usa questo certificato. Questa funzione impiega gli stessi strumenti della funzione di ricerca oggetti implementata negli elementi di configurazione di un'appliance.

Visualizzazione dei tunnel VPN

La gestione dei tunnel VPN nel NETASQ UNIFIED MANAGER offre una nuova funzione per aggiungere/rimuovere tunnel VPN configurati sull'appliance.

Gestione della rubrica

A seguito dell'accorpamento delle applicazioni di gestione sui prodotti NETASQ (UNIFIED MANAGER, REAL-TIME MONITOR e EVENT REPORTER), è stato migliorato il formato dei file di backup del progetto (modalità Global Administration) per standardizzare il formato della rubrica nelle applicazioni di gestione dei prodotti NETASQ.

La conversione del formato del file è trasparente nella nuova versione del NETASQ UNIFIED MANAGER. Aprendo un file di backup (con estensione *.gap) creato con una versione precedente, questo verrà automaticamente convertito al nuovo formato eseguendo il backup della nuova versione del NETASQ UNIFIED MANAGER (modalità Global Administration).

NETASQ REAL-TIME MONITOR

Applicazione SEISMO

Il NETASQ REAL-TIME MONITOR mostra informazioni relative alle applicazioni rilevate da SEISMO. Ulteriori informazioni si possono trovare nella sezione dedicata ai miglioramenti apportati a NETASQ SEISMO.

Allarmi critici

Per poter configurare il motore ASQ nella modalità di rilevazione delle intrusioni, il pannello "Allarmi" nell'applicazione NETASQ REAL-TIME MONITOR presenta ora informazioni aggiuntive inerenti gli allarmi critici. Questi allarmi vengono lanciati quando il sistema di prevenzione delle intrusioni rileva pacchetti sensibili, per i quali è stato configurato nella modalità di rilevazione delle intrusioni.

Interfaccia grafica

Il NETASQ REAL-TIME MONITOR dispone ora di una nuova interfaccia grafica. Su tutti i pannelli (SEISMO, Host, VPN tunnels, ecc.) è ora possibile:

- Lanciare una ricerca con criteri avanzati
- Ridimensionare le colonne per adattarle al contenuto (menu contestuale nelle colonne della tabella)
- Filtrare la tabella di presentazione secondo i criteri selezionati (menu contestuale della tabella)

Inoltre, la visualizzazione dello stesso pannello su diverse appliance è stata consolidata nella stessa schermata in fondo alla pagina. I dati relativi ad un'appliance sono accessibili cliccando sulla scheda e selezionando l'appliance.

Presentazione delle informazioni

Il NETASQ REAL-TIME MONITOR presenta numerose modifiche nella visualizzazione delle informazioni.

- La schermata **Alarms** contiene ora due nuove colonne (Sensitive and IP protocol).
- La schermata **SEISMO** presenta nuove informazioni, trattate nella sezione dedicata ai miglioramenti di NETASQ SEISMO.
- La schermata **Host** contiene nuove colonne nel pannello principale (Users, Applications e Events) e nei pannelli della finestra con le informazioni dettagliate ("Vulnerability", "Information" rinominata "Events", "Services" rinominata "Applications", nuova scheda "Alarms").
- La schermata **Quarantine** si chiama ora "List of dynamic addresses" e contiene due tabelle - "Quarantine" e "Whitelist".
- La schermata **VPN tunnels** non presenta più una panoramica dettagliata: le informazioni sono ora mostrate nelle nuove colonne della panoramica generale - "Source address", "Destination address", "Incoming SPI", "Outgoing SPI", "Incoming ReqId" e "Outgoing ReqId".
- La generazione delle informazioni nella schermata **Services** è stata migliorata: i dati relativi ai proxy sono mostrati separatamente, la voce relativa ai proxy è stata sostituita da 4 nuove voci - HTTP Proxy, SMTP Proxy, POP3 Proxy e FTP Proxy.

- La schermata **VPN policy** contiene nuove colonne ("Source address", "Source gateway address", "Destination gateway address", "Destination address" e "Negotiated Security Associations").
- Nella schermata **Logs**, le tabelle con i diversi tipi di log sono state modificate onde visualizzare più informazioni.

Strumenti di navigazione

L'applicazione NETASQ REAL-TIME MONITOR fornisce strumenti di navigazione che permettono un accesso più rapido alle informazioni tramite il menù contestuale.

- Spostamento del comando **"Update OS manually"** dalla schermata **Hosts** alla scheda "Software" nella schermata SEISMO.
- Aggiunta del comando **"Delete the host from SEISMO"** per disabilitare la registrazione dell'avvio di un host come evento da parte di SEISMO.
- Rimozione del comando **"View vulnerability"** nel pannello "Vulnerability" della finestra "hosts".
- Aggiunta del comando **"View hosts with the same vulnerability"** nel pannello "Vulnerability" della finestra "hosts".
- Aggiunta del comando **"List all hosts using this application"** nel pannello "Application" della panoramica dettagliata degli "hosts".
- Aggiunta del comando **"List this application's vulnerabilities"** nella tab "Application" della schermata Hosts.
- Aggiunta del comando **"Force the application of this server"** nel pannello "Application" della schermata Hosts.
- Rimozione del comando **"View information"** nel pannello "Events" della panoramica dettagliata degli "hosts".
- Aggiunta del comando **"List hosts with the same event"** nel pannello "Events" della panoramica dettagliata degli "hosts".
- Aggiunta dei comandi **"View packet that raised alarm"**, **"Filter by this value"** e **"Copy to clipboard"** nel pannello "Alarms" della panoramica dettagliata degli "hosts".
- Aggiunta dei comandi **"View outgoing SPI logs"**, **"View incoming SPI logs"**, **"View outgoing VPN policy"** e **"View incoming VPN policy"** nella panoramica dei tunnel VPN.
- Aggiunta del comando **"View tunnel"** nella schermata VPN policy.

Gestione degli indirizzi

Il NETASQ REAL-TIME MONITOR può sfruttare lo stesso elenco indirizzi del NETASQ UNIFIED MANAGER.

Inoltre, una funzione di ricerca permette di trovare velocemente le appliance.

Accesso alle appliance nella modalità console

L'applicazione NETASQ REAL-TIME MONITOR consente di accedere alle appliance nella modalità console (comandi CLI).

NETASQ EVENT REPORTER

Supporto di informazioni raccolte nei log

A seguito dell'implementazione delle nuove funzionalità, i prodotti NETASQ offrono nuovi file log per gli eventi. L'applicazione NETASQ EVENT REPORTER offre inoltre il trattamento dei seguenti dati:

- Proxy FTP
- Plugin SIP

Inoltre, a seguito dell'aggiunta dei nuovi tag per il miglioramento dei dati generati nei moduli SEISMO e IPSec, il NETASQ EVENT REPORTER è stato aggiornato per mostrare questi dati.

Gestione della raccolta e dell'archiviazione delle informazioni

Il modulo NETASQ COLLECTOR offre nuove funzioni per l'archiviazione delle informazioni. È ora possibile:

- Definire la cartella di destinazione per gli archivi
- Configurare l'archiviazione come opzionale

Disabilitare la reportistica automatica

Il modulo NETASQ AUTOREPORT dà ora la possibilità di abilitare o disabilitare la produzione di uno o più report.

Gestione degli indirizzi

Il NETASQ EVENT REPORTER può sfruttare lo stesso elenco indirizzi dell'applicazione NETASQ UNIFIED MANAGER.

Inoltre, una funzione di ricerca permette di trovare velocemente le appliance.

Aggiornamento dei database

L'applicazione NETASQ EVENT REPORTER dispone della nuova versione del database PostgreSQL (versione 8.3).

Nota: Essendo ancora supportata la versione 8.2 del PostgreSQL, non è necessaria la migrazione del database in fase di aggiornamento del NETASQ EVENT REPORTER. L'aggiornamento non è però consigliabile qualora si migri dalle versioni 7.x alla 8.0.

NETASQ UPDATER

L'applicazione NETASQ UPDATER può essere configurata tramite un'interfaccia grafica, accessibile dal menu Start di Windows Start menu (Start -> All Programs -> NETASQ -> NETASQ Updater -> netasqupdaterui).

SSL VPN

Il modulo SSL VPN dei prodotti NETASQ è dotato di tre nuove funzioni:

- Migliore supporto di Javascript (AJAX, ...)
- Supporto di OWA 2003 e 2007 nella modalità premium
- Supporto di Lotus Notes

Il perfezionamento della gestione dei link ipertestuali va oltre il semplice supporto dei Javascript, e consiste in una completa revisione del meccanismo di gestione di tali link. Essendo il linguaggio Javascript eseguito dalla postazione client e contenendo potenziali link ipertestuali, il componente SSL VPN analizza e modifica le funzioni del linguaggio al fine di modificare i link ipertestuali per indirizzarli al portale SSL VPN.

Potale di autenticazione: supporto dell'olandese

È ora disponibile la versione in lingua olandese del portale di accesso ai prodotti NETASQ.

Proxy SMTP

L'integrazione del modulo antispam nel proxy SMTP dei prodotti NETASQ (analisi euristica e/o DNS blacklist) è stata migliorata per abilitare il blocco delle e-mail. Senza portare le e-mail a destinazione, il proxy SMTP risponde al server SMTP remoto indicando che il messaggio è stato rifiutato e considerato spam. In questo modo l'utente non riceverà il messaggio nella posta in entrata.

Questa funzione, configurabile tramite il NETASQ UNIFIED MANAGER, è comparabile al servizio già esistente che stabilisce le soglie di fiducia. Una volta impostate le soglie di criticità secondo i valori di fiducia assegnati alle e-mail, è possibile impostare la soglia oltre la quale i messaggi verranno rifiutati anziché dotati di tag.

Aggiornamento attivo

Reindirizzamento HTTP

Il modulo di aggiornamento automatico è in grado di interpretare i comandi di reindirizzamento HTTP. In tal modo, è possibile accedere direttamente ai file attraverso le URL, ma è possibile inoltrare gli update NETASQ anche ad un altro server in caso di elevato traffico.

Ripristino dell'aggiornamento (Serie U e appliance dalla F200 alla F5500)

La procedura di aggiornamento automatica è stata migliorata per permettere un recupero automatico dei dati in caso di fallimento dell'aggiornamento dei moduli dinamici.

Firme contestuali SEISMO

La procedura di aggiornamento automatico comprende le firme contestuali del modulo NETASQ SEISMO.

Gestione dei dialup

Il modulo di gestione delle connessioni con il provider internet è stato aggiornato. Oltre alla maggior stabilità delle connessioni PPP, PPOE e PPTP, questa modifica ha riguardato principalmente i tunnel L2TP che richiederanno l'esplicita impostazione di un possibile link di backup.

SNMP Agent

Gestione degli allarmi

Il modulo SNMP offre ora una migliore gestione dell'invio dei trap. È possibile attivare gli allarmi per gruppi (ASQ / System events) che prevedono il lancio di soli allarmi critici e configurare allarmi minori per ogni gruppo.

ID del motore

La sicurezza dell'identificativo del motore SNMP v3 (engineID) è stata rinforzata al fine di codificare il valore in una gamma da 5 a 32 byte. I dispositivi NETASQ non accettano più solo valori compresi tra 16 (10000) e $2^{32} - 1$ compreso.

Nota: I valori inferiori a 16 verranno modificati con l'aggiunta di tanti 0 quanti sono necessari per coprire il numero di byte mancanti. Ad esempio, il valore 1 (0x1) sarà convertito in 16 (0x10000).

Servizio DHCP

Il modulo DHCP è stato aggiornato per assicurare maggiore stabilità.

NS-BSD

Sistema operativo

La nuova versione dei prodotti NETASQ integra un importante aggiornamento del sistema operativo NS-BSD, offrendo:

- Miglior gestione delle risorse
- Nuovo supporto hardware (carte di rete e hard disk SATA)
- Perfezionamento dei trattamenti multiprocessore
- Aggiornamento del modulo di monitoraggio del servizio
- Interfaccia seriale che può essere configurata fino a 115200 bauds (valore di default 9600 bauds)

Visualizzazione delle informazioni di interfaccia

Lo stato delle interfacce viene visualizzato in modalità console dopo il login ed offre la seguente panoramica:

```
F200XB000010599999: FW F200-B (M / INTERNAL)
Firewall software version 8.0.0
Port    name  NS-BSD    state    address
1       out   fxp1      up       10.2.6.254/16
2       in    fxp0      up       10.2.6.254/16
3       dmz3  fxp2      no-link  10.2.6.254/16
4       dmz2  fxp3      no-link  172.254.0.1/16
```

```
F200XB000010599999>
```

8.0.0 Vulnerabilità rimosse

ClamAV

Il modulo ClamAV è stato modificato onde correggere una vulnerabilità inerente al buffer overflow (CVE 2008-5050) che in che in alcuni contesti può causare un denial of service sull'applicazione o sull'esecuzione del codice.

Nota: Già dalla versione 6.2 il server ClamAV operava senza alcun privilegio.

8.0.0 Bug fixes

ASQ

Blocco dell'opzione SACK-Permitted

Riferimento assistenza: 16434

Il motore ASQ è stato modificato onde permettere ai server di inviare pacchetti SYN/ACK con l'opzione SACK-Permitted anche se quest'ultima non è stata richiesta dal client.

SEISMO

Visualizzazione delle e-mail in Outlook 2007

Riferimento assistenza: 16281

Risolti i problemi di visualizzazione delle e-mail inviate da SEISMO in Outlook 2007.

IPSec VPN

Ritrasmissione dei pacchetti IKE

Riferimento assistenza: 16055

Risolti i problemi nella ritrasmissione dei pacchetti IKE comparsi occasionalmente nelle configurazioni NAT-T.

Ripristino dell'elenco revoche

Riferimento assistenza: 17076

Corretto il modulo IPSec che caricava una lista di revoche ripristinata da un'operazione di backup (.na file).

Proxy

Avvio del proxy senza antivirus

Riferimento assistenza: 14763

Corretta l'applicazione dell'elemento di configurazione che permette al proxy di avviarsi senza il modulo antivirus.

Miglioramenti delle richieste ICAP-REQMOD

Riferimento assistenza: 15836

Migliorata la gestione delle richieste POST per il metodo REQMOD nel protocollo ICAP.

Gestione dei segmenti "double data" nelle risposte HTTP

Riferimenti assistenza: 15385 e 16057

In alcune implementazioni, l'ultimo segmento di dati nelle risposte HTTP (linee contenenti il carattere '0') viene raddoppiato. Il proxy non blocca più questo tipo di risposta.

Nota: L'allarme "Additional data at end of reply" (identificativo 150 nel contesto HTTP) deve essere impostato su "Pass" in modo che il sistema di prevenzione delle intrusioni lasci passare l'ultimo segmento doppio dei dati.

Stabilità del proxy POP3

Riferimento assistenza: 16509

Migliorata la stabilità del proxy POP3 e corretto lo sporadico rifiuto della richiesta di creare nuove connessioni.

Autenticazione

Pagina di rinnovo dei certificati

La pagina di rinnovo dei certificati utente è nuovamente accessibile.

Alta disponibilità

Scambio improvviso

Risolto lo scambio improvviso occasionalmente verificatosi durante la procedura di sincronizzazione.

Sistema

Verifica dei file di configurazione DHCP

Riferimento assistenza: 14439

Il file di configurazione DHCP generato con `builddhcp (/var/dhcpd.conf)` viene ora controllato prima che il servizio sia attivato.

Falle di memoria nell'events manager

Riferimento assistenza: 15716

Risolve le falle di memoria generate dal riavvio dell'events manager (`eventd daemon`).

Fuso orario iracheno

Riferimento assistenza: 16373

La gestione del fuso orario per l'Iraq è stata aggiornata sui prodotti NETASQ, non adottando questo Paese l'ora legale.

Rimozione della VLAN

Riferimenti assistenza: 16228 e 16229

Risolve la sospensione del link VLAN in alta disponibilità quando una VLAN viene rimossa.

Stabilità dei daemons

Riferimento assistenza: 16367

Corretti i daemons che si riavviano dopo l'aggiornamento.

Gestione della "subversion"

Riferimento assistenza: 16496

Corretto l'errore che non consentiva di assegnare i servizi di una subversion al protocollo TCP.

Inizializzazione dell'interfaccia

Riferimento assistenza: 16962

Risolti i problemi di inizializzazione dell'interfaccia di rete causanti uno stato di "amnesia" risolvibile solo riavviando l'appliance.

NETASQ UNIFIED MANAGER

Visualizzazione del menu di quarantena ASQ

Riferimento assistenza: 16041

Risolto l'errore nella visualizzazione dell'etichetta del menu di quarantena all'apertura della finestra della prevenzione contro le intrusioni.

Modifica di allarmi che non possono essere modificati

Riferimento assistenza: 16238

Risolto l'errore che permetteva – tramite la rotellina del mouse – di impostare il valore di un allarme che non poteva essere modificato.

Visualizzazione della durata delle DHCP

Riferimento assistenza: 16433

Corretta la visualizzazione della durata delle sessioni DHCP.

Informazioni su Kaspersky

Le informazioni riguardanti Kaspersky sono visualizzate solo sulle appliance dotate della relativa licenza.

8.0.0.1 Vulnerabilità rimosse

ClamAV

Il modulo ClamAV è stato aggiornato onde correggere una vulnerabilità presente sui file JPEG (Secunia Advisory SA32926) che, in alcuni contesti, poteva cagionare un denial of service dell'applicazione

8.0.0.1 Bug fixes

Sistema

Inizializzazione crittografata per il syslog

Riferimento assistenza: 17194

Risolto il blocco dei daemon switchati a seguito dell'invio di log su un syslog criptato.

8.0.0.2 Bug fixes

Sistema

Stabilità di sistema

Riferimento assistenza: 17381

Il sistema è stato aggiornato per correggere l'instabilità concomitante al trattamento del traffico IPSEC.

Suite di amministrazione

Raccolta dei log per la serie U

Riferimento assistenza: 17423

La nuova versione della suite di amministrazione include una licenza standard del modulo LogCollector che permette di raccogliere le informazioni nei log dei prodotti della Serie U (entro il limite numerico permesso dalla licenza del prodotto).

8.0.0.2 Problemi noti

Interfacce di rete

Limite VLAN e MTU

Se da un lato il valore MTU associato ad una interfaccia fisica supporta fino a 1500 byte, le VLAN ad esso associate non possono presentare un valore MTU che superi i 1496 byte.

Esiste una soluzione temporanea a questo problema, documentata nella knowledge database.

Questo problema sarà risolto definitivamente nella release 8.0.1.

Pubblicazione ARP di connessioni PPTP

Il servizio PPTP non imposta la pubblicazione ARP per l'indirizzo IP del client PPTP.

Questo problema sarà risolto definitivamente nella release 8.0.1.

Autenticazione

Dimensione del token SPNEGO

I token SPNEGO con header superiori a 3 kilobytes non vengono gestiti correttamente.

Questo problema sarà risolto definitivamente nella release 8.0.1.

Sistema

Ripristino dei backup della Serie F sulle appliance della Serie U

Poiché alcuni modelli di F50 e F60 hanno interfacce IN e OUT invertite, il ripristino delle loro configurazioni sulla nuova versione delle appliance manterrà tale inversione. Quest'anomalia si verifica solo con backup realizzati con una versione del software precedente alla 8.0.0.

Questo problema sarà risolto definitivamente nella release 8.0.1.

Funzioni della versione 8.0.1

Motore ASQ

Perfezionamento dell'analisi del protocollo TCP

Sono state aggiunte nuove analisi comportamentali del protocollo TCP al motore di prevenzione contro le intrusioni ASQ. Tali analisi consentono di proteggere la rete da falle nel protocollo TCP, che in alcuni casi potrebbero favorire attacchi DoS (denial of service).

Ad esempio, l'uso delle opzioni TCP che consentono di ridurre la finestra, possono dar luogo ad un'accumulazione di dati sul server TCP (HTTP, FTP, ecc) senza che gli stessi vengano trasmessi al client che li aveva richiesti. Query multiple da parte dei client che originano tale comportamento potrebbero causare una saturazione delle risorse del server. Per evitare tale situazione, il motore di prevenzione contro le intrusioni identificherà tale abuso e chiuderà le connessioni di conseguenza.

Inoltre, quando un client TCP moltiplica duplicati di comandi ACK che non contengono alcun dato, il server potrebbe essere obbligato ad adeguare il proprio comportamento (algoritmo RENO) e quindi consumare più risorse. Il motore IPS tratta questi pacchetti singolarmente per evitare che il server si saturi.

NETASQ UNIFIED MANAGER

Prevenzione contro le intrusioni: Durata della validità di finestre TCP ridotte

Con l'applicazione NETASQ UNIFIED MANAGER è possibile configurare il periodo di validità di finestre TCP ridotte. Questo parametro può essere modificato nel pannello delle impostazioni avanzate, dove si può definire il lasso di tempo dopo il quale scadranno le connessioni stateful per il modulo IPS.

Prevenzione contro le intrusioni: Attivazione della protezione avanzata per il protocollo TCP

Il NETASQ UNIFIED MANAGER consente di abilitare o disattivare la funzione di protezione avanzata sul protocollo TCP. A questo parametro si accede attraverso il pannello per la configurazione delle connessioni stateful nel modulo IPS.

8.0.1 Vulnerabilità rimosse

PKI

Il modulo OpenSSL è stato aggiornato per correggere una vulnerabilità inerente al controllo inesatto di firme DSA dalla formattazione inadeguata (CVE 2008-5077).

Cache DNS

Una vulnerabilità identificata sul modulo della cache DNS ne riduce il livello di sicurezza. Sono due le correzioni applicate ai dispositivi NETASQ :

- Qualora si ricevano più query su una stessa registrazione, solo una query sarà trasmessa al DNS.
- Il collegamento col plugin DNS è stato imposto per tutte le connessioni in uscita che passano attraverso il proxy.

8.0.1 Bug fixes

Sistema

Banca dati di oggetti

Riferimento assistenza: 16669

In alcune configurazioni inerenti a banche dati di oggetti che contengono un numero elevato di elementi che richiedono una risoluzione DNS dinamica, l'accesso a tali oggetti veniva interrotto ogni volta che il server DNS non era disponibile. Abbiamo perfezionato la gestione della disponibilità dei server DNS durante la risoluzione dei nomi.

Interruzione del traffico su desincronizzazione

Riferimento assistenza: 14972

Corretta la desincronizzazione che alcune volte poteva causare l'interruzione del traffico. Tale interruzione aveva luogo qualora entrambi i dispositivi subissero deterioramenti.

Wizard di configurazione web-based in Polacco

Riferimento assistenza: 16956

Il wizard di configurazione dei dispositivi NETASQ è stato tradotto in Polacco.

Active Update

Impossibilità di aggiornare DNSRBL e Vaderetro

Riferimento assistenza: 16905

L'errore che cagionava l'occasionale fallimento dell'update delle blacklist di mail server (DNS RBL) e del motore antispam Vaderetro è stato corretto.

SSL VPN

Blocco dei tag HTML con parametri troppo grandi

Riferimento assistenza: 16098

I tag HTML con dimensione superiore a 64K bytes fare di più il blocco del download della pagina.

Proxy

Interruzione del motore antivirus

Riferimento assistenza: 16342 e 16626

Corretto il comportamento anomalo del motore antivirus che causava talvolta l'interruzione della scansione antivirus.

Blocco di connessione e ICAP

Riferimento assistenza: 16590

Proxy HTTP ora restituisce una pagina di errore e un esplicito log, quando il server ICAP non era disponibile.

Proxy FTP

Riferimento assistenza: 17477

Corretto l'invio di comandi FTP PASV e PORT tra il client FTP ed il dispositivo NETASQ in configurazione passiva e, in configurazione attiva, per il traffico in uscita.

Interfaccia di rete

Valore VLAN ed MTU

Riferimento assistenza: 17465

Per le VLAN configurate sui prodotti della serie U, è ora possibile impostare il valore MTU fino a 1500 byte. In precedenza, poiché il valore MTU di un'interfaccia fisica non poteva superare i 1500 byte, le VLAN ad esso associate non potevano avere un valore maggiore di 1496 byte.

Broadcast ARP delle connessioni PPTP

Riferimento assistenza: 16937

L'anomalia nel broadcast ARP delle connessioni PPTP su un ampio numero d'interfacce è stata corretta.

Ripristino della configurazione di rete

Riferimento assistenza: 17326

Il ripristino di un backup condotto con la versione 7 sulla versione 8 non causa più modifiche della configurazione di rete.

Autenticazione

SPNEGO: dimensionamento token

Riferimento assistenza: 16679

Il buffer di lettura è stato incrementato per supportare token sovradimensionati. Le dimensioni massime supportate per i token KERBEROS ora di 20 KB, contro i 3 KB precedenti.

Mancata applicazione del CRL aggiornato

Riferimento assistenza: 17187 e 15946

L'applicazione di un CRL aggiornato non richiede più il reboot del servizio di autenticazione per l'autenticazione dei tunnel IPsec.

Parametri dei certificati

Riferimento assistenza: 16771

Ora è possibile ricercare i certificati all'interno di una directory LDAP sia su indirizzi email sia sui campi CN o UID. Nelle versioni precedenti tale ricerca poteva essere condotta solo sul campo e-mail.

Nota: questa funzione può essere abilitata in modalità console, modificando il file `/usr/Firewall/ConfigFiles/auth`.

```
[SSL]
CertificateIdentifier=uid | mail | cn
```

Inoltre i dispositivi NETASQ ora accettano i certificati X.509 che contengano nell'oggetto dei campi DC (domainComponent).

Revoca del certificato

Riferimento assistenza: 17518

La migrazione dalla versione 7 alla versione 8 poteva bloccare la funzione di revoca utenti e quindi la creazione di nuove liste di certificati revocati. È stato corretto l'errore generato dallo script per la migrazione.

Autenticazione KERBEROS

Riferimento assistenza: 15878

I sistemi ora supportano anche eventuali caratteri speciali Latin-1 presenti nelle password KERBEROS.

Portale d'autenticazione: supporto del polacco

Riferimento assistenza: 17251

Il portale d'autenticazione dei prodotti NETASQ è ora disponibile anche in lingua polacca.

NETASQ REAL-TIME MONITOR

Avvio dal NETASQ UNIFIED MANAGER

Riferimento assistenza: 17416

Corretto l'errore di avvio dell'applicazione NETASQ REAL-TIME MONITOR dal NETASQ UNIFIED MANAGER per dispositivi che appaiono nell'elenco indirizzi.

8.0.1.1 Vulnerabilità rimosse

ClamAV

Il motore antivirus ClamAV è stato aggiornato, onde correggere due vulnerabilità (Secunia Advisory SA34566 e SA34612) che in alcuni contesti possono causare un denial of service dell'applicazione o quando si esegue il codice.

Nota: Già dalla versione 6.2 il server ClamAV opera senza alcun privilegio.

8.0.1.1 Bug Fixes

Interfacce di rete

Configurazione del client DynDNS

Riferimento assistenza: 18008

Corretto l'errore che si verificava in sede di configurazione del client DynDNS.

Proxy

SMTP

Riferimento assistenza: 18128

Il proxy SMTP presentava a volte comportamenti tali per cui alcune connessioni venivano bloccate. Questa anomalia è stata corretta.

Active Update

Notifica di errore durante l'aggiornamento

Riferimento assistenza: 18408

La notifica "Kaspersky error" compariva a volte senza però alcun impatto sul processo di aggiornamento lanciato dalla console. Questo messaggio non appare più.

Aggiornamento della banca dati Kaspersky

Il modulo di aggiornamento della banca dati delle signature di Kaspersky è stato modificato per gestire una banca dati di maggiori dimensioni.

Modifica degli indirizzi dei server

Gli indirizzi IP dei server per l'aggiornamento sono stati modificati. La nuova versione corregge quindi i file di configurazione aggiornando tali indirizzi.

IPsec VPN

DPD: IPsec SAs (security associations) non autorizzate

Riferimento assistenza: 17739

Impiegando il servizio d'identificazione dei dead peer senza abilitare NAT-T, le IPsec SAs non venivano rilasciate quando si riscontrava un dead peer. Questa anomalia è stata corretta.

Miglioramento della stabilità

Riferimento assistenza: 17930

Modificato il modulo IPsec VPN per migliorarne il comportamento qualora impiegato in un ambiente con multiprocessori e numerosi client mobili.

Pacchetti IKE_FRAG con formato inadeguato

La ricezione di pacchetti IKE_FRAG con formato inadeguato causava a volte la chiusura del Daemon Raccoon. Questa anomalia è stata corretta.

Funzioni della versione 8.0.2

Motore ASQ

Nuove analisi protocollari HTTP

Abbiamo aggiunto nuove analisi comportamentali per il protocollo http al motore di prevenzione contro le intrusioni ASQ. Con queste nuove analisi abbiamo perfezionato la protezione dei web server contro una falla che poteva dar luogo, in alcuni casi, all'interruzione dei servizi (DoS).

Questa falla consiste nell'invio di solo una parte dei dati di una query HTTP (attacco di tipo « Slowloris »). Il web server che riceve tale query parziale alloca delle risorse per poterla trattare ma non può rilasciarle finché non ha ricevuto tutti i dati della query. La moltiplicazione di richieste di questo tipo cagiona molto velocemente una saturazione delle risorse del server. Per evitare tale situazione, il motore di prevenzione contro le intrusioni individua tale comportamento abusivo e di conseguenza chiude la connessione.

Nuovi contesti di analisi

Sono stati creati 18 nuovi contesti protocollari per l'applicazione delle signature contestuali di protezione su dati relativi. Tali contesti saranno impiegati progressivamente e visibili non appena sarà stata aggiunta la prima signature.

Nuova protezione del protocollo SIP

Il plugin SIP é stato modificato per incrementare la protezione sullo header « Max-Forwards ». Il valore del campo viene analizzato e gli header « Max-Forwards » duplicati vengono attualmente bloccati. È stato anche aggiunto l'allarme minore « invalid value in SIP header Max-Forward ». Nella configurazione standard questo allarme (ID 153) è bloccante.

8.0.2 Vulnerabilità rimosse

IPSEC

Il modulo IPSEC é stato aggiornato per correggere una vulnerabilità di pacchetti creati in modo tale da dar luogo, in alcuni contesti, ad un Denial of Service.

NTP

Il modulo NTP é stato aggiornato per correggere una vulnerabilità in caso di attivazione dell'autenticazione attraverso « Autokey » (CVE-2009-1252) che in alcuni casi consentiva l'esecuzione di codici dannosi da remoto.

Nota : i dispositivi NETASQ non sono vulnerabili a questa falla.

8.0.2 Bug Fixes

Motore ASQ

Congelamento del sistema

Riferimento assistenza: 17985, 18391 et 18563

Un problema di gestione dei percorsi nel motore ASQ a volte cagionava il congelamento del sistema. Questa anomalia é stata corretta.

Allarme ASQ sul protocollo HTTP

Riferimento assistenza: 17896

L'allarme ASQ « Possible buffer overflow on URL » emesso a volte qualora si individuasse un riferimento ad una pagina "parent" nella URL (../..) é stato corretto.

Kernel crash

Riferimento assistenza: 17791

La generazione di un allarme sensibile qualora il plugin generico associato veniva disattivato cagionava un crash del kernel. Questa anomalia é stata corretta.

SIP Plugin: header VIA

Riferimento assistenza: 18715

La presenza di uno spazio nello header VIA non origina più l'allarme « Bad VIA field in SIP ».

DNS Plugin: errore del log

Riferimento assistenza: 18225

L'errore del log sul campo « dstname », per alcune connessioni del proxy HTTP destinate all'interfaccia di « loopback » dei dispositivi è stato corretto.

Routing avanzato

Riferimento assistenza: 18682

La verifica della disponibilità di un router testando un gruppo di hosts (gruppo di verifica) é stata corretta.

Tabella hosts

Riferimento assistenza: 18869

L'algoritmo per la gestione della saturazione della tabella degli host è stato perfezionato.

TTL multicast

Riferimento assistenza: 19040

Il valore del campo TTL in un pacchetto multicast che attraversa un bridge non sarà più modificato.

Query HTTP con caratteri ASCII a 8 bit

Query HTTP contenenti caratteri ASCII a 8 bit ora vengono bloccate e viene emesso l'allarme "Invalid HTTP protocol (8 bits in the query)". Query di questo tipo possono essere accettate, qualora si abiliti l'opzione "passonfail". In particolare, questo allarme viene generato su connessioni HTTP fittizie generate da Skype.

SEISMO

Estrazione per server Apache2

La versione del modulo mod_ssl per I server Apache v2.x viene ora estratta correttamente.

Proxy

Chiusura del proxy HTTP esplicito

Riferimento assistenza: 17904

L'attivazione del filtro URL OPTENET cagionava a volte la chiusura del proxy HTTP esplicito. Questo errore é stato corretto.

Autenticazione attraverso il proxy HTTP esplicito

Riferimento assistenza: 17584

L'impossibilità di ridirigere clients con un IP non protetto o non noto da un proxy esplicito al portale di autenticazione é stata risolta. Ora i client collegati ad un'interfaccia non protetta o non nota saranno indirizzati al portale di autenticazione in base al profilo di autenticazione esterno.

Il profilo standard del proxy HTTP dovrà essere quindi specificato nella configurazione (HTTPDefault).

Autenticazione e indirizzamento ad un proxy esterno

Riferimento assistenza: 19098

Nel caso in cui la configurazione di un proxy HTTP richieda l'indirizzamento del traffico verso un proxy esterno con l'autenticazione dell'utente non veniva inviato l'header "Proxy Authorization". Questo errore, che aveva conseguenze solo su gruppi di utenti con nomi troppo lunghi, è stato corretto.

Filtro URL: indirizzamento al portale

Riferimento assistenza: 15326

L'indirizzamento alla pagina del portale non funzionava in caso fossero implementate delle regole di filtro URL molto specifiche. Questo errore é stato corretto.

Antivirus: Passaggio da ClamAV a KasperskyEmbedded

Riferimento assistenza: 18987, 18995, 19010 and 19016

Il passaggio dal motore ClamAV al motore KasperskyEmbedded per modelli dotati solo di memoria flash della serie F è stato perfezionato. Il processo non richiede più l'impiego di specifici comandi né il riavvio del dispositivo.

Timeout della connessione del proxy HTTP

Abbiamo aggiunto un timeout per la generazione di connessioni del proxy HTTP. Di conseguenza il proxy consentirà al browser di mostrare la pagina “host could not be reached” invece di attendere una risposta da un sito remoto.

Il valore del timeout può essere impostato nel file /usr/Firewall/ConfigFiles/HTTPProxy/0X:

```
[config]
TimeoutSrvConnect=integer /*default value is 20 sec*/
```

ICAP: Gestione dei log nel caso di un reindirizzamento

Le sessioni ora vengono registrate correttamente con il messaggio “URL has been changed by ICAP server” qualora un server ICAP modifichi una URL (per reindirizzamento ad una pagina d’errore).

ICAP: Modifica della porta TCP

La modifica della porta TCP nelle risposte ICAP per il reindirizzamento a server HTTP che ascoltano un’altra porta ora viene gestita correttamente.

Proxy FTP: Passive mode

Riferimento assistenza: 17847

L’attivazione della modalità passiva su un client FTP mentre la modalità attiva è stata imposta al server viene ora gestita correttamente.

Perfezionamento proxy FTP

Il proxy FTP è stato migliorato per fornire ulteriore protezione qualora vengano aperte varie connessioni “child”. Il nuovo messaggio “Old child connection removed” è quindi stato aggiunto per indicare quando il proxy cancella i duplicati delle connessioni.

Proxy FTP: comando EPRT con parametri IPv6

Quando nel comando EPRT si trova un parametro IPv6, la connessione non può più essere chiusa. Il proxy ora risponde con il messaggio “502 error in parameters of EPRT command”.

Proxy POP3: meccanismo “Keepalive”

Il meccanismo “Keepalive” che consente di mantenere attive le connessioni POP3 durante la scansione antivirus è stato perfezionato.

Proxy POP3: Data pipelining

Perfezionamento della gestione del data pipelining.

Log dei proxy duplicati

I log delle connessioni per i proxy che ascoltano porte non standard (21,25, 80 e 100) non saranno più duplicati.

Antispam: Gestione del carattere di tabulazione

Riferimento assistenza: 17977

La lista bianca ora viene applicata correttamente anche agli header "From" che contengono un carattere di tabulazione.

Antispam: grado di spam sconosciuto

Riferimento assistenza: 18158

Quando uno dei server RBL DNS non risponde, il grado di spam di un messaggio poteva essere indicato come "sconosciuto". Questa correzione riguarda il calcolo del grado di spam, che ha ora luogo senza tenere in considerazione i server non raggiungibili.

ClamAV antivirus

In alcuni casi il motore ClamAV ci mette meno ad inviare i propri risultati ai proxy.

Autenticazione

Chiusura del daemon durante l'autenticazione SSO

Riferimento assistenza: 18219 and 18675

L'accesso diretto alla pagina di autenticazione SSO poteva dar luogo alla chiusura inaspettata del daemon. Questo errore è stato corretto.

Signature degli applet sul portale

Riferimento assistenza: 18297

Appena scaduto il loro certificato, gli applet SrpAuth e XvpnClient sono stati ricertificati.

Eccezione Java

Riferimento assistenza: 18248 and 18828

L'eccezione Java che ha avuto luogo in alcuni casi durante l'aggiornamento della password è stata risolta.

Pagina di errore SPNEGO

Nel caso di impossibilità di effettuare un'autenticazione SPNEGO, la pagina di errore veniva ricaricata ogni 3 secondi. Ora l'utente viene ridiretto dalla pagina di errore alla pagina di login.

VPN SSL

Riscrittura Cookie

Riferimento assistenza: 18072 and 18677

La funzione di riscrittura dei cookie di grosse dimensioni è stata corretta.

Indirizzamento al Citrix Presentation Server

Riferimento assistenza: 17110

Il supporto per il reindirizzamento di pagine nel Citrix PresentationServer 4.5 é stato migliorato.

OWA 2003: Cartelle condivise

Riferimento assistenza: 17387

Migliorato il supporto delle cartelle condivise di OWA 2003.

Configurazione di accessi web multipli con un host singolo

Riferimento assistenza: 18376

Configurare due accessi web con lo stesso oggetto "host" non é più possibile. Questa configurazione difatti non é autorizzata poiché non funziona correttamente. È necessario quindi indicare uno host specifico per ogni accesso SSL VPN.

Porta d'ascolto specifica

Riferimento assistenza: 17436

Il modulo SSL VPN é ora in grado di ascoltare una porta TCP specifica.

CSS personalizzato

La personalizzazione del modello CSS per la serie U funziona correttamente.

VPN IPSEC

Caricamento certificato o CRL vuoti

Riferimento assistenza: 18134

Il problema emerso in fase di caricamento della configurazione della VPN via IPS quando si impiegano certificati o CRL vuoti é stato risolto.

Crash del kernel

Riferimento assistenza: 17931

Il crash del kernel che ha avuto luogo qualora si abilitasse la cache SPD con troppo poche o troppe registrazioni è stato corretto.

Nota: la cache SPD é una funzione di ottimizzazione non abilitata nella configurazione standard ed accessibile esclusivamente attraverso la command line del dispositivo.

Tcpdump sull'interfaccia enc0

Riferimento assistenza: 17636

Il traffico cifrato o decodificato individuato sull'interfaccia enc0 viene ora visualizzato correttamente. Gli header ESP per il traffico in uscita non vengono più mostrati.

File Dump dall'interfaccia enc0

Riferimento assistenza: 17937

La cattura di traffico cifrato o decodificato in un file (opzione -w) sull'interfaccia enc0 é stata corretta.

IPSec SA inutilizzate

Le IPSec SA inutilizzate vengono cancellate all'effettivo scadere delle SA rispettive e non più all'80% della durata.

Pianificazione di eventi "Keepalive"

Quando si riavviava un dispositivo, la pianificazione degli eventi "Keepalive" non veniva più presa in considerazione. Questo errore è stato corretto.

Sistema

HA: Eliminazione connessioni ripristinate

Riferimento assistenza: 18094

Dopo un switchover in alta disponibilità, alcune connessioni ripristinate venivano accidentalmente eliminate. Questo aveva luogo qualora la connessione fosse accettata da una regola di filtro applicata all'interfaccia in ingresso. Questo errore è stato corretto.

HA: Status active/active dopo aver riavviato il dispositivo passivo

Riferimento assistenza: 18035 and 18372

I dispositivi installati in cluster HA non ripartono in modalità attiva se hanno individuato un mero "heartbeat" invece che la presenza di una sessione serverd. Tale comportamento dava luogo all'avvio del cluster in modalità attivo/attivo sebbene il dispositivo passivo fosse stato riavviato.

HA: Affidabilità del cambiamento dello stato

Riferimento assistenza: 18062 and 18686

Miglioramento del cambiamento dello stato dei dispositivi in cluster HA.

HA: risoluzione nome DNS

Il dispositivo passivo in un cluster non tenterà più di risolvere il nome DNS di host dinamici (objectsync).

Invio di log criptati

Riferimento assistenza: 18270

L'invio di log criptati a diversi server syslog è stato corretto.

Configurazione log standard

Riferimento assistenza: 19044

La configurazione standard dei log è stata modificata. I log ora sono distribuiti per il 100% dello spazio sul disco.

Routing dinamico

Riferimento assistenza: 18651

Corrett l'errore in fase di caricamento del file di configurazione.

Pianificazione delle policy

Riferimento assistenza: 18020

La disabilitazione della pianificazione delle policy (slots) ora viene applicata correttamente.

Ripristino tramite chiavetta USB stick

Riferimento assistenza: 18903

Corretto l'errore di avvio del ripristino di una configurazione tramite back-up effettuato su chiavetta USB.

Ripristino della configurazione

Riferimento assistenza: 17326

Ripristinare una configurazione nella versione 7 di un dispositivo non fallirà più in assenza di una banca dati LDAP nel file di backup. La gestione degli errori che si possono verificare durante il ripristino è stata perfezionata.

PKI: Rimozione delle CRL

Quando un certificato relativo ad un CA importato viene cancellato, la CRL associata sarà cancellata anch'essa correttamente.

Test sull'integrità della configurazione

I seguenti moduli sono ora parte del controllo dell'integrità della configurazione:

- Antivirus
- Active Update
- Antispam
- HA

NETASQ Unified Manager

Plugin SSL: indentificazione Skype

Riferimento assistenza: 18084

La checkbox che consente di abilitare o disabilitare l'identificazione di Skype funziona correttamente.

Accesso alla guida

Riferimento assistenza: 18469

Corretto l'errore di accesso alla guida.

LDAP wizard: campo DC

Riferimento assistenza: 18006

Il campo di testo "DC" del wizard per la creazione di un LDAP interno sta per "Domain Component" e non più per "Domain Country".

Informazioni licenza

Riferimento assistenza: 18153

La generazione di informazioni sulle licenze dei dispositivi che non dispongono di un'opzione POP3 ora viene gestita correttamente.

Filtro URL e nome oggetti

Riferimento assistenza: 18037

Oggetti i cui nomi iniziano con "on" o "off" vengono ora visualizzati correttamente nelle regole di filtraggio web.

Crash durante l'avvio

Riferimento assistenza: 18655

I crash che si verificava in fase di avvio qualora venisse caricato un file XML malamente formattato è stato corretto.

Allocazione di spazio per i log

Riferimento assistenza: 18649

Lo spazio allocato per i log non viene ricalcolato qualora si identifichi un errore, specialmente quando lo spazio totale disponibile per l'archiviazione viene superato. Ciò nonostante l'amministratore di sistema verrà informato qualora la distribuzione dello spazio allocato superi il 100%.

Global Administration: menu "Tool" (strumenti)

Riferimento assistenza: 18400

Il messaggio di errore che compariva nei dispositivi F5000 durante l'avvio dell'applicazione NETASQ REAL-TIME MONITOR ed EVENT REPORTER (menu contestuale "Tools") è stato corretto.

NETASQ REAL-TIME MONITOR

Gestione dello spazio per log FTP e SSL VPN

Riferimento assistenza: 18042

Lo spazio disponibile e già in uso per log FTP e SSL VPN viene ora visualizzato correttamente.

Modifica dei criteri di filtro

L'applicazione di filtri contenenti più criteri non sarà più modificata qualora si cambi l'elenco dei dispositivi visualizzato.

NETASQ EVENT REPORTER

Inizializzazione della password

Riferimento assistenza: 17749

Il wizard di installazione non suggerisce più di cambiare la password per accedere alla banca dati.

NETASQ UPDATER

Aggiornamento del servizio

L'aggiornamento dell'Administration Suite da una versione 8 precedente non includeva il servizio NETASQ UPDATER. Questa anomalia, che non riguardava invece gli aggiornamenti dalla versione 7 alla versione 8, è stata corretta.

8.0.2 Problemi noti

Interfacce di rete

VLANs collegate ad un'interfaccia disabilitata

Riferimento assistenza: 14891

Le VLANs collegate ad un'interfaccia disabilitata non funzionano correttamente se l'interfaccia primaria stata configurata via DHCP.

Un modo per evitare questo problema é configurare un indirizzo IP statico per l'interfaccia primaria.

Pubblicazione ARP su un bridge disattivato

Riferimento assistenza: 17719

Un problema di apprendimento ARP può verificarsi qualora la prima interfaccia di riferimento di un bridge sia stata disattivata. Dopo aver eseguito il comando di configurazione di rete alcuni host risultano appartenere all'interfaccia disattivata fino a quando non vengono registrati su un'altra interfaccia. Durante questo periodo il traffico verso tali host potrebbe essere bloccato.

Un modo per evitare tale situazione é abilitare tale interfaccia anche se non connessa o utilizzata.

Autenticazione

Nome dell'oggetto identico al nome del dominio Windows

Riferimento assistenza: 13734

Configurare un oggetto "host" con lo stesso nome del dominio Windows non consente al dispositivo di reperire correttamente l'elenco degli utenti.

IPSEC VPN

Gestione delle policy "Bypass"

Riferimento assistenza: 17873

Per aggiungere o cancellare una policy VPN "Bypass" è necessario disattivare e riattivare lo slot VPN. Fare un semplice "reload" dello slot VPN porta la policy alla fine della SPD, ove, per un corretto funzionamento, dovrebbe essere posta in cima.

Sistema

Velocità dell'interfaccia seriale

Riferimento assistenza: 16806

Il messaggio di sistema "more tty-level Buffer Overflow" appariva a volte nella console sui dispositivi U1100, U1500 e U6000. Ciò significa che i caratteri vengono inviati più velocemente di quanto l'hardware possa leggerli.