

NETASQ UTM Versione 7.0.9

Punti salienti della versione 7

- NETASQ SEISMO
- Nuova banca dati per l'archiviazione dei log
- Nuovi strumenti per la gestione dei dispositivi
- SSL VPN versione 2

Nota: Questo documento raggruppa le informazioni sulla versione 7.0 e le release minori 7.0.1. e 7.0.2., 7.0.3, 7.0.3.1, 7.0.4., 7.0.5, 7.0.6, 7.0.7, 7.0.8. Informazioni specifiche relative alla versione 7.0.9 si trovano invece alla fine del documento (a partire da pagina 33).

Attenzione: le modalità di reazione del modulo antivirus su alcuni modelli F25 e F50 é stata modificata, Si raccomanda esplicitamente di verificare le configurazioni che impiegano la VPN IPsec con certificati (cfr. "7.0.3: Bug fixes" a pagina 17).

Funzioni della versione 7.0

NETASQ SEISMO

Questo strumento di analisi perimetrale in tempo reale genera file di background per qualunque host presente sulla rete in base ad un profilo di configurazione specifico. Le informazioni raccolte in questi file vengono impiegate per identificare le vulnerabilità presenti sui diversi host. Gli strumenti di NETASQ sono stati modificati per poter presentare, riordinare e correlare questi dati nel modo migliore. Scoprite ulteriori dettagli su NETASQ SEISMO consultando la scheda tecnica del prodotto.

NETASQ Administration Suite

Composizione

I dispositivi di NETASQ impiegano ora un singolo insieme di strumenti gestionali (Administration Suite) che combina le variazioni apportate alle versioni precedenti.

- NETASQ UNIFIED MANAGER sostituisce sia lo strumento precedente, sinora noto come Firewall Manager, sia la console di gestione Global Administration.
- NETASQ REAL-TIME MONITOR sostituisce il Firewall Monitor.
- NETASQ EVENT REPORTER sostituisce il Reporter ed il Reporter Pro. Entrambi vengono attualmente distinti in base alla licenza.
- NETASQ Updater è un nuovo strumento che consente di aggiornare gli allarmi, le informazioni sulle vulnerabilità e i file di sistema.

Software per l'installazione

La nuova Administration Suite è dotata di un singolo assistente per l'installazione dalle dimensioni ottimizzate.

VERSIONE 7.0.9

Funzioni	Nessuna
Correzione errori	Minore
Correzione vulnerabilità	Maggiore

AGGIORNAMENTO

Versione minima richiesta

6.3.0

Alta disponibilità (HA): versione minima richiesta

6.3.2

Livello delle modifiche 6.3 -> 7.0

Archiviazione log	Rivista
SSL VPN	Rivisto
Administration Suite	Maggiore
ASQ	Maggiore
QoS	Maggiore
IPSec VPN	Minore
Report automatico	Minore
Alta disponibilità (HA)	Minore
Filtri/NAT	Nessuna

COMPATIBILITÀ VERSIONE 7.0

F25	F25-B e superiori
F50	F50-C e superiori
F60	Tutti i modelli
F200	Tutti i modelli
F500	Tutti i modelli
F800	Tutti i modelli
F1000	Tutti i modelli
F1200	Tutti i modelli
F2000-F2500	Tutti i modelli
F5000-F5500	Tutti i modelli

Compatibilità

Prima di installare l'Administration Suite è necessario che sia disponibile una componente MSI 3 (per runtime VC++ 2005). Si può accedere a questo modulo attraverso il Windows Update.

NETASQ UNIFIED MANAGER

Combinazione di Firewall Manager e console gestionale Global Administration

Il Firewall Manager e la console gestionale Global Administration sono state combinate dando vita al NETASQ UNIFIED MANAGER, che opera in due modi distinti: La modalità "Manager" e la modalità "Global Administration". Per passare da una modalità all'altra basta selezionare la propria preferenza nel menu Options - Preferences.

Visualizzazione dei firewall nella modalità "Global Administration"

L'amministrazione dei dispositivi UTM di NETASQ con la versione 7.0 è molto più semplice grazie alla possibilità di accedere alla visualizzazione dei singoli firewall NETASQ installati (nella panoramica generale o topologica - cliccare con il tasto destro del mouse e selezionare "Manage"). La "Firewall View" offre tutte le funzioni necessarie per configurare un dispositivo UTM di NETASQ allo stesso modo in cui questo compito veniva assolto in precedenza dal Firewall Manager.

Elenco degli indirizzi

Il formato dell'elenco degli indirizzi è stato aggiornato in modo da renderlo identico ai progetti della Global Administration (.gap). Con la nuova versione il file con l'elenco degli indirizzi viene archiviato in C:\Documenti e Impostazioni\<NOMEUTENTE>\Dati applicazioni\Netasq\AS\7.0 invece che nella cartella di installazione dell'applicazione. Per importare l'elenco degli indirizzi prodotto con la versione 6.3 basta selezionare dal menu "File - address book" e poi "Import" nella modalità Manager o "File - Import address book" nella modalità Global Administration.

Attivazione automatizzata del monitoraggio UTM

È possibile attivare / disattivare il monitoraggio automatico per ogni singolo dispositivo, sia modificando il valore contenuto nella colonna "monitoring" della panoramica generale, sia cliccando con il tasto destro del mouse su uno dei dispositivi UTM presenti nella panoramica topologica.

La licenza del NETASQ UNIFIED MANAGER

Il NETASQ UNIFIED MANAGER viene venduto con una licenza per l'impiego con 5 dispositivi UTM. Tuttavia questa restrizione non viene più applicata al numero di dispositivi UTM contenuti nel progetto. L'amministratore sarà quindi in grado di importare l'intero elenco degli indirizzi indipendentemente dal quantitativo di dispositivi inclusi nell'elenco. La restrizione trova invece applicazione nel numero di prodotti visualizzabili nella panoramica topologica o nel numero di dispositivi che possono essere aggiunti al parco macchine installate.

NETASQ REAL-TIME MONITOR

Nuova applicazione

Il NETASQ REAL-TIME MONITOR è un'applicazione nuova di monitoraggio in tempo reale che sostituisce il Monitor presente nella versione 6.3 ed inferiori. Oltre ad offrire tutte le funzioni del Monitor 6.3 e a presentarsi in un look completamente nuovo, il NETASQ REAL-TIME MONITOR integra molte nuove funzioni, descritte qui di seguito.

Panoramica

Con una operatività multi-appliance perfezionata rispetto al suo predecessore, il NETASQ REAL-TIME MONITOR offre una panoramica dei dispositivi UTM sotto forma di un elenco che viene generato sia in base alle informazioni incluse nell'elenco degli indirizzi, sia in base alle registrazioni condotte manualmente. Informazioni quali la versione installata, lo stato degli aggiornamenti automatici o dell'antivirus vengono presentate con immediatezza nella panoramica.

Bacheca dettagliata

Per ogni dispositivo UTM gestito dal NETASQ REAL-TIME MONITOR è disponibile una bacheca che consente di visualizzare informazioni dettagliate sui sistemi (CPU, memoria), potenziali incidenti rilevati o sullo stato dei sistemi ad alta disponibilità (HA). La bacheca fornisce quindi una visuale dettagliata dello stato di qualsivoglia dispositivo UTM NETASQ ed è accessibile dalla schermata principale cliccando sul tasto destro del mouse.

Integrazione di NETASQ SEISMO

Il NETASQ REAL-TIME MONITOR offre inoltre informazioni sullo stato di NETASQ SEISMO. La panoramica principale consente di visualizzare il numero delle vulnerabilità identificate su tutte le reti. Le informazioni di SEISMO sono ordinate per vulnerabilità o per tipo di informazioni raccolte. La panoramica sugli host è stata totalmente rivista onde migliorare l'intuitività delle informazioni raccolte per un dato host (vulnerabilità, servizi identificati, connessioni, ecc).

Infine la visualizzazione degli allarmi integra le informazioni fornite da SEISMO. Lasciando il cursore sulla fonte o la destinazione di un dato allarme appariranno le informazioni sulle vulnerabilità presenti su uno specifico host.

Navigazione tra le diverse schermate

È possibile navigare tra le diverse modalità di visualizzazione del NETASQ REAL-TIME MONITOR in diversi modi. Le svariate informazioni presenti nella bacheca forniscono collegamenti ipertestuali alle relative descrizioni dettagliate. Attraverso SEISMO, nella finestra di visualizzazione di host e allarmi, è possibile accedere alla funzione di navigazione cliccando con il tasto destro del mouse.

Filtraggio e riorganizzazione

Il NETASQ REAL-TIME MONITOR consente di filtrare e/o riordinare le informazioni in diverse modalità di visualizzazione: panoramica generale, allarmi, SEISMO, utente, host, interfaccia, IPSec VPN, visualizzazione delle policy e dei log.

Monitoraggio dei dispositivi con versione precedente

Il NETASQ REAL-TIME MONITOR può essere impiegato con tutti i prodotti UTM di NETASQ con la versione 5.1 e superiori.

NETASQ EVENT REPORTER

Nuovo nome

Il Firewall Reporter ora è il NETASQ EVENT REPORTER, che racchiude le funzioni del Reporter, la raccolta di informazioni ("Collector") e la reportistica automatica ("Autoreport").

Nuova banca dati

Il nuovo NETASQ EVENT REPORTER si basa su un server PostgreSQL 8.2 ed è dotato di una banca dati interamente ristrutturata. La banca dati attuale è una banca dati relazionale e la struttura delle tabelle è stata completamente rivista.

Nota: Non è necessario installare il server contenente la banca dati sul controller di dominio.

Migrazione della banca dati

Alla luce delle modifiche apportate alla struttura della banca dati, le informazioni raccolte con la versione 6.3 non possono essere utilizzate direttamente con il Collector 7.0. Tuttavia il Collector 7.0 consente di raccogliere i log dei dispositivi UTM di NETASQ a partire dalla versione 5.1. Al contrario il Collector 6.3 o inferiore non potrà radunare i log delle appliance UTM con versione 7.0. Si possono quindi considerare diversi scenari per la migrazione, ad esempio installare il Collector 7.0 e raccogliere le informazioni dei sistemi UTM 6.3 ed inferiori. Non appena si conclude il periodo di raccolta log più lungo, chiudere il vecchio Collector ed aggiornare i dispositivi UTM con la versione 7.0.

Archiviazione e rotazione dei dati

Il Collector consente di far ruotare i dati raccolti in modo automatico. A questa funzione si accede dal menu "Tools - Manage Collector" della finestra "Database". Una volta concluso il periodo definito dall'amministratore, i dati verranno esportati automaticamente in formato syslog (file di testo) ed archiviati nella cartella dell'applicazione: C:\Documents and Settings\<USER>\Application Data\Netsq\AS\7.0\LogCollRel\Syslog_Dump.

Collector: impostazioni avanzate

L'amministratore può assegnare una specifica priorità al servizio di raccolta dei log. A questa funzione si accede dal menu "Tools - Manage Collector" della finestra "Advanced modifications".

Visualizzazione "Grafici" con il Reporter

L'interfaccia del Reporter consente di generare nuovi grafici: impiego della CPU, tracking delle regole QoS, vulnerabilità segnalate da SEISMO e dati correlati a SEISMO. Tali grafici offrono una panoramica dell'evoluzione di tali valori in un dato periodo. Ciò consente, ad esempio, di monitorare il traffico a lungo termine, senza degradarne la performance creando una

apposita regola di monitoraggio QoS.

Nota: aggiornando il sistema alla versione 7.0, i dati dos vengono integrati automaticamente nei log impiegati dal NETASQ EVENT REPORTER. Con l'aggiornamento, l'amministratore disporrà quindi di nuove informazioni senza un suo previo intervento.

Variazioni della reportistica automatica

La banca dati del generatore di report automatico è stata modificata e consente di creare rapporti che contengano elenchi "Top 100" e non solo "Top 10". È possibile generare rapporti in base ai seguenti log: amministrazione, autenticazione, IPSec VPN, SSL VPN e statistiche. Inoltre è possibile integrare i grafici nei report (richiede una specifica configurazione). I rapporti vengono archiviati prima di essere inoltrati. La funzione "Execute now" attiva la creazione immediata di un report schedato in modo da ottenere il rapporto desiderato prima del termine stabilito.

NETASQ Updater

Ora l'Administration Suite include un nuovo strumento che aggiorna automaticamente le guide relative agli allarmi e le informazioni su SEISMO.

Aggiornamenti

Formato degli aggiornamenti

Il formato degli aggiornamenti era già stato modificato con la versione 6.3. Grazie a tale variazione gli aggiornamenti constano di diversi pacchetti indipendenti. In sede di aggiornamento ad una nuova versione ("major release") verranno installati tutti i pacchetti. In sede di aggiornamento di singoli elementi ("minor release") verranno installati solo i pacchetti modificati.

Solo 1 reboot

È necessario riavviare il sistema una sola volta, non più due come nelle versioni precedenti.

Motore antivirus Kaspersky incluso negli aggiornamenti NETASQ

Il motore antivirus Kaspersky ora è incluso negli aggiornamenti NETASQ. Quindi non è più necessario scaricare specificamente l'aggiornamento Kaspersky. Per attivare la funzione Kaspersky antivirus è necessario installare semplicemente la licenza corrispondente e selezionarla dal menu antivirus del NETASQ UNIFIED MANAGER.

ASQ

Assegnazione di porte standard ai plug-in di analisi protocollare

Ad ogni plug-in di analisi di protocollo di ASQ sono state assegnate "porte standard" quale specifica proprietà. Di conseguenza i protocolli a cui si riferisce il plug-in verranno analizzati su tutte le porte indicate nelle proprietà. Precedentemente invece era necessario creare una regola di filtraggio esplicita per forzare l'assegnazione di un dato plug-in ad una specifica porta.

Nota: per semplificare la migrazione, l'aggiornamento alla versione 7.0 non presenterà alcuna indicazione sulla porta da analizzare. Qualora si resettino i prodotti con versione 7.0 alla configurazione standard, ogni plug-in conterrà l'indicazione di una porta standard (ad esempio porta 80 http per il plug-in di analisi http).

Assegnazione automatica di un profilo ASQ

Sono disponibili 4 profili di configurazione di ASQ da impiegare automaticamente per i collegamenti con reti non sicure (connessioni in uscita, generalmente verso l'Internet). Allo stesso modo è possibile assegnare un profilo a connessioni in ingresso provenienti dalla stessa rete non sicura (in genere da Internet e diretti ad un server presente nella rete aziendale).

Nota: l'aggiornamento alla versione 7.0 prevede l'applicazione del profilo 00 a tutte le connessioni. Qualora si resettì il prodotto con versione 7.0, il profilo 01 verrà assegnato a tutte le connessioni in uscita. Il livello di sicurezza per gli allarmi previsto da questo profilo è impostato su "Internet" onde ridurre ulteriormente il rischio di falsi positivi.

Nuovo plug-in di analisi sul protocollo SSL

Il motore d'analisi ASQ è stato dotato di un nuovo plug-in di analisi protocollare SSL che controlla la validità della connessione SSL. Le analisi condotte su tale protocollo consentono altresì di bloccare eventuali connessioni che impieghino algoritmi di cifratura troppo deboli ed l'eventuale traffico non cifrato che segue una negoziazione SSL. A tale plug-in sono state associate

diverse categorie di firme contestuali, disponibili tramite "Active Update".

Nota: Il plug-in SSL blocca l'accesso al portale per l'autenticazione sui prodotti che non dispongono di una solida cifratura. Per consentire l'accesso al portale, il plug-in SSL va configurato in modo da autorizzare algoritmi di cifratura "deboli". (vedasi sezione 7.0.1: problem noti, pagina 10).

Nuovo MySQL

Questo plug-in applicativo consente di identificare automaticamente il protocollo MySQL (porta standard 3306/TCP) e fornisce al modulo SEISMO tutte le informazioni sul server MySQL rinvenuto.

HTTP plug-in perfezionato

Le analisi delle URL si sono evolute in modo da adattarsi al progressivo allungamento degli indirizzi web di domini pubblici. Sono stati inseriti 3 nuovi parametri per l'individuazione di vulnerabilità dovute a buffer overflow: URL, riferito alle dimensioni dell'indirizzo senza parametrizzazione; QUERY, riferito alla dimensione totale dell'elenco dei parametri; ARGUMENT, riferito alle dimensioni massime di ogni argomento. Il secondo miglioramento apportato concerne l'individuazione di errate codifiche delle URL. Qualora si sospetti un una doppia codifica, l'indirizzo web verrà decodificato una seconda volta e le firme contestuali verranno applicate nuovamente. Lo scopo di tale modifica è di migliorare l'efficienza delle analisi riducendo drasticamente il numero di falsi positivi generati da alcuni siti pubblici che contengono indirizzi non validi.

SMTP plug-in perfezionato

Il plug-in SMTP è stato modificato onde consentire al motore SEISMO di trarne le informazioni rilevanti. Di conseguenza le analisi protocollari assicurano che i campi necessari a SEISMO siano conformi agli standard e che vengano emessi allarmi di "invalidità del protocollo" ogni qual volta si identifichi una anomalia.

Qualità del Servizio (QoS)

Valori di riferimento e assegnazione

Con la versione 7.0 cambia il modo in cui si impiega il valore di riferimento qualora sia stata impostata almeno una regola di assegnazione di banda nella policy attiva. Tale valore di riferimento (a cui si accede dal menu "General" nella finestra relativa alla QoS) sarà applicato come limite condiviso da tutte le regole QoS (Qid), incluse le regole di monitoraggio. Tale cambiamento si è reso necessario onde garantire l'efficacia della assegnazione di banda. È quindi particolarmente importante impostare tale valore per consentire un corretto funzionamento delle diverse regole.

SSL VPN

Nuovo percorso per il server SSL VPN

Il percorso del server SSL VPN è stato completamente modificato ed impiega esclusivamente la porta TCP 443. Sia l'accesso ad internet, sia gli applet java impiegheranno il protocollo SSL per collegarsi ai prodotti NETASQ sulla porta TCP 443. Tale perfezionamento interessa particolarmente il modo in cui i link vengono modificati nelle pagine accessibili tramite SSL VPN. Quindi i link relativi a pagine web vengono modificati, mentre prima venivano lasciati come erano.

Nota: In sede di aggiornamento di apparecchi con la versione 6.3, le regole di filtraggio implicite contenute nel modulo SSL VPN dei dispositivi UTM NETASQ vengono cancellate. L'unica regola implicita presente nella versione 7.0 riguarda il server per l'autenticazione (autorizzazione all'accesso alla porta TCP 443).

Server Presentazione Citrix

Tramite SSL VPN di NETASQ è possibile accedere all'applicazione del server di presentazione Citrix. Per accedere a tale server sarà necessario effettuare una prima impostazione ("Other server - Citrix"), che consente di incapsulare il traffico dell'applicazione, ed una seconda impostazione ("HTTP server") per configurare il portale d'accesso. Una volta condotte tali operazioni, l'utente dovrà lanciare l'applet Java e selezionare le applicazioni che desidera utilizzare dal collegamento ipertestuale al portale Citrix. A causa dei cambiamenti apportati al traffico applicativo sull'applet Java, sarà possibile configurare un singolo server Citrix sul dispositivo UTM di NETASQ.

Accesso Web di Outlook (OWA)

La correzione dei link relativi interessa anche la compatibilità OWA e rende necessario modificare il campo "User-Agent" se

l'utente desidera accedere ad un server OWA. Questa impostazione si effettua nella finestra di configurazione dello SSL VPN. Le pagine OWA verranno quindi visualizzate in modalità di compatibilità e non più in modalità "Premium".

Nota: Aggiornando un apparecchio con la versione 6.3, verrà aggiunta automaticamente la funzione "Rewrite User-Agent". Una volta terminato l'aggiornamento, gli utenti accederanno ad OWA ma sempre in modalità di compatibilità.

IPSec VPN

NAT-T: supporto di vari "peers" dietro ad un singolo indirizzo IP

Il modulo IPSec VPN è stato perfezionato onde supportare diversi tunnel remoti provenienti dallo stesso indirizzo IP. Questa situazione si verifica spesso quando si impiegano diversi client VPN per collegarsi ad una risorsa centrale da una singola connessione internet (p.es. da un aeroporto o albergo).

Autenticazione

Nuovo look della piattaforma

La piattaforma web di NETASQ ha subito un "restyling" in base alla nuova corporate Identity delle applicazioni NETASQ.

Piattaforma di autenticazione in Spagnolo

La piattaforma di autenticazione è disponibile in inglese, francese, tedesco, italiano, portoghese e spagnolo. La configurazione del Vostro browser determinerà la lingua della piattaforma.

Autenticazione SRP e traslazione degli indirizzi

Qualora gli utenti impieghino il metodo di autenticazione SRP, l'applet Java userà il nome DNS della piattaforma di autenticazione al posto dell'indirizzo IP del firewall. Ciò comporta che l'autenticazione SRP possa essere utilizzata anche qualora l'indirizzo IP del dispositivo UTM di NETASQ sia diverso dall'indirizzo IP identificato dal browser (generalmente qualora l'indirizzo sia stato modificato da un altro dispositivo).

Rimozione dei limiti di lunghezza del nome di gruppi di utenti

Nelle versioni precedenti la lunghezza del nome di tutti i gruppi a cui appartenevano gli utenti era limitata a 127 caratteri.

Autenticazione Kerberos

L'autenticazione Kerberos impiega generalmente UDP ma si appoggia su TCP per le richieste con troppi parametri. Ora il server di autenticazione passa automaticamente da UDP a TCP quando si identificano tali richieste.

HTTP Proxy

Miglioramento dei tempi di visualizzazione delle pagine web

L'analisi delle pagine web è stata modificata (in special modo il "pipelining" ed il "chunking") con un netto incremento della velocità con cui le pagine web verranno visualizzate nel browser.

Impiego del gruppo URL "antivirus_bypass"

Il gruppo di URL "antivirus_bypass" viene impiegato automaticamente da tutti i profili di HTTP proxy per determinare un elenco di siti che non devono essere scansati dall'antivirus. Le pagine web nell'elenco vengono trasmesse direttamente al browser attraverso il proxy, senza alcun buffering. Questo gruppo contiene una registrazione standard: il sito di aggiornamento di Windows. Gli aggiornamenti condotti tramite "Windows Update" hanno luogo con un download di file parziali (il browser richiede frazioni di file) e l'analisi antivirus bloccherebbe un tale comportamento.

Nota: Questo gruppo viene creato automaticamente in fase di aggiornamento. Non è necessario includerlo in una policy di filtraggio web ai fini dell'impiego su proxy HTTP.

Active Update

Impiego di un proxy HTTP con autenticazione

È possibile condurre gli aggiornamenti automatici attraverso un proxy HTTP, che richiede solo un nome utente ed una

password.

Configurazione dei parametri avanzati "Check signature"

Gli aggiornamenti di NETASQ sono dotati di firma digitale per verificare l'autenticità e l'integrità dei file scaricati. Qualora tale parametro sia disattivato, il modulo "Active Update" non controllerà più alcuna firma digitale con la conseguenza che non sarà in grado di scaricare ed installare un aggiornamento firmato.

Agente SNMP

Nuovo MIB di NETASQ

L'agente SNMP di NETASQ contiene nuovi MIB che forniscono informazioni sul sistema (l'equivalente del comando "*system property*"), sullo stato di Active Updates ("*monitor autoupdate*"), sulle policy attive ("*monitor policy*") e sullo stato dei servizi ("*monitor service*").

SNMP v3: cifratura AES

L'agente SNMP è ora in grado di cifrare le informazioni che invia impiegando un algoritmo di cifratura AES.

Avvisi per mail

Elenco destinatari

Con la versione 7.0 la modalità di invio dei messaggi di sistema è stata rivista totalmente. È disponibile un menu per la posta elettronica accessibile direttamente dal menu principale del NETASQ UNIFIED MANAGER. L'amministratore può configurare un elenco di destinatari o specifiche registrazioni nella banca dati utente. Tali elenchi vengono impiegati per inviare allarmi o notifiche di eventi del sistema e i rapporti generati automaticamente da SEISMO.

Nota: In sede di aggiornamento il gruppo "Administrators" viene creato automaticamente e contiene tutti gli indirizzi presenti sul dispositivo prima dell'aggiornamento.

Template di posta elettronica

L'amministratore può modificare i diversi tipi di messaggi inviati da un dispositivo UTM NETASQ. Le mail sulle iscrizioni o sui report concernenti le vulnerabilità possono essere totalmente configurate.

NS-BSD

Gateway standard: load balancing ed alta disponibilità (HA)

È possibile creare un elenco di router sui quali distribuire le connessioni in uscita. In precedenza tale funzione era disponibile esclusivamente per modem e connessioni dial-up. Ora l'elenco include sia i router statici sia i gateway presenti sull'interfaccia DHCP. Riguardo all'interfaccia DHCP è necessario che l'amministratore faccia attenzione a non configurare 2 interfacce per lo stesso access provider. Difatti, l'elenco di gateway potrebbe contenere due indirizzi IP identici, senza essere in grado di differenziarli. Per poter risolvere tale problema, si consiglia di posizionare il router tra il dispositivo UTM di NETASQ ed uno dei due server DHCP.

Server SLD

Il server SLD sostituisce l'autenticazione (authd), lo SSL VPN (xvpnd) ed i server dei wizard per l'installazione (webd).

Alta disponibilità

Rimozione dell'interfaccia seriale sIO

Il supporto della funzione di alta disponibilità tramite collegamento seriale non viene più fornito dalla versione 5.0. Con la versione 7.0 tale interfaccia viene rimossa in modo permanente, disattivando totalmente la funzione su link seriale.

Aggiornamento trasparente

Un dispositivo UTM con versione 7.0 può comunicare esclusivamente con apparecchi dotati della versione 6.3.2 e superiori. Dopo l'aggiornamento il collegamento con gli apparecchi dotati di una versione inferiore verrà interrotto.

7.0: Vulnerabilità rimosse

ClamAV

Il modulo ClamAV è stato modificato onde correggere una vulnerabilità sul parser OLE2 (CVE-2007-2650) che in alcuni contesti può causare un denial of service sull'applicazione ClamAV.

Nota: Già dalla versione 6.2 il server ClamAV operava senza alcun privilegio (utente "nobody").

Libreria C-Ares

La libreria di conversione del server dei nomi (DNS) impiegata dalla banca dati degli oggetti è stata aggiornata per rafforzare la creazione di valori casuali impiegati nell'identificazione di una query. Il plug-in di analisi DNS impiega diverse metodologie di protezione efficienti per combattere lo sfruttamento di questo tipo di vulnerabilità.

7.0.1: Funzioni

ASQ: nuova evasione di URL identificata

Sono stati identificati I tentativi di evasione nella codifica di caratteri ASCII (%uFFxx) in UTF-8 che generano l'allarme "Evasion using %u encoding".

Backup

In modalità avanzata è possibile effettuare il backup della configurazione dei gruppi di destinatari dei messaggi di allerta.

Assistenza (sysinfo)

Riferimento assistenza: 14453

La modalità di visualizzazione delle informazioni sui profili di ASQ è stata modificata. Il Profilo 00 viene visualizzato integralmente ma di seguito vengono proposte solo le differenze tra il Profilo 00 e gli altri profili.

Filtraggio URL: elenchi personalizzati

I filtri URL di NETASQ consentono di definire server privati dai quali ottenere aggiornamenti sugli elenchi di URL. In questa modalità operativa il campo "Check signature" (verifica firme) é deselezionato (secure=0). La verifica delle firme include ora un controllo dell'integrità che non veniva condotto sui server privati.

Example: master1 file, urlgroup section

```
[urlgroup]
master1=5
master2=5
last=5
subsys=1
master1_md5=b2c56a12db8c68baa9000e89e9f6bf29
master2_md5=b2c56a12db8c68baa9000e89e9f6bf29
```

Active Update controllerà l'esistenza di una riga md5 nel file master e testerà l'integrità di ogni categoria nella banca dati delle URL (qualora esistente), ogni qual volta venga scaricato un aggiornamento.

NETASQ REAL-TIME MONITOR: log IPSec VPN

Sono stati aggiunti nuovi campi ai log su VPN IPSec -"rete locale", "rete remota" e "ruolo". Il valore assegnato al campo "ruolo" può essere "initiator" (indica che un dispositivo UTM ha inizializzato un tunnel) o "responder" (quando il tunnel non parte dal dispositivo UTM indicato).

7.0.1: Bug fixes

SSL VPN: scaricare file pesanti (> 1 MB)

Riferimento assistenza: 14408

È possibile scaricare file pesanti (> 1MB) attraverso tunnel VPN SSL .

Autenticazione

Errore di autenticazione Kerberos

Riferimento assistenza: 13219

Qualora sia attivata l'autenticazione trasparente ma questa non venga impiegata dall'utente, lo stesso viene deviato su un'altra modalità di autenticazione. Se il client impiegato era IE 6.0 ed il metodo di autenticazione a cui veniva ridiretto era Kerberos, l'autenticazione non veniva condotta correttamente. Ora, qualora si verifichi un tale situazione, compare un pop-up di dialogo che consentirà l'autenticazione.

Autenticazione senza banca dati LDAP configurata

In alcuni casi l'autenticazione può fallire qualora non sia stata configurata alcuna banca dati LDAP sul dispositivo UTM NETASQ.

SNMP

Perdita di memoria

Riferimento assistenza: 14321

Nelle versioni precedenti, qualora non fosse stata configurato alcun percorso standard, alcuni messaggi di allerta SNMP non potevano essere inviati, cagionando una perdita di memoria di qualche byte.

Messaggi di allerta per firme contestuali

In alcuni casi gli allarmi SNMP con informazioni fornite dall'analisi delle firme contestuali potevano contenere messaggi errati.

Sistema

Percorsi statici

Riferimento assistenza: 13671

Risolto il problema legato all'aggiornamento / rimozione dei percorsi statici.

NTP

Riferimento assistenza: 14320

Il client NTP opera ora normalmente sui dispositivi F2500/F5500.

NETASQ UNIFIED MANAGER

Oggetti: servizi UDP

I servizi UDP vengono visualizzati correttamente.

Oggetti: nomi che cominciano con il carattere '-'

Ora sono autorizzati anche gli oggetti i cui nomi iniziano con il carattere '-' seguito da cifre.

Active Update

Riferimento assistenza: 14424

La frequenza degli aggiornamenti può essere configurata correttamente indipendentemente dal formato della data impiegato dal sistema operativo.

Modalità Global Administration

Riferimento assistenza: 14421

Il ripristino dell'ultimo backup nella data attuale viene selezionato correttamente.

Lingua della guida sugli eventi di sistema

La guida relativa agli eventi di sistema viene visualizzata nella lingua corretta.

Finestra licenze

Le informazioni sulle licenze vengono visualizzate correttamente.

Finestra SEISMO

In alcuni casi selezionare una riga del profilo di SEISMO causava un'interruzione dell'applicazione.

NETASQ EVENT REPORTER

Esportazione dei log

L'applicazione NETASQ EVENT REPORTER si destabilizzava qualora si tentasse di esportare un file di log aperto in un'altra applicazione.

Collector

Supporto di dati in formato italiano.

7.0.1: Vulnerabilità rimosse

ClamAV

Il modulo ClamAV è stato aggiornato onde correggere una vulnerabilità presente sul parser html (Secunia SA-26530) che, in alcuni contesti, poteva cagionare un denial of service dell'applicazione ClamAV.

Nota: Già dalla versione 6.2 il server ClamAV operava senza alcun privilegio (utente "nobody").

7.0.1: Problemi noti

ASQ: analisi del protocollo SSL e portale per l'autenticazione

I prodotti destinati a Paesi con i quali non è stato siglato alcun accordo specifico verranno forniti con un sistema "EXPORT 3". Questo sistema è dotato esclusivamente di algoritmi di cifratura deboli. Il plug-in di analisi SSL non consente l'impiego di questo tipo di algoritmi nella sua configurazione standard, negando quindi l'accesso al portale per l'autenticazione. Per poter accedere al portale sarà necessario modificare la configurazione del plug-in di analisi del protocollo SSL in modo tale da consentire l'impiego di tali algoritmi.

7.0.2 : Vulnerabilità rimosse

LDAP

Rimosso eventuale denial of service su server LDAP dovuto a queries LDAP prodotte ad hoc (CVE-2007-5707).

SNMP

Rimosso eventuale denial of service sul modulo SNMP dovuto a queries GETBULK prodotte ad hoc (CVE-2007-5846).

7.0.2 : Funzioni

NS-BSD

Autenticazione - Portale per l'accesso remoto

L'applet di autenticazione Java e per il tunnel SSL VPN è stato ricertificato per aggiornarne la validità.

ASQ

Plugin SSL

La configurazione del plugin SSL sui prodotti forniti in modalità "EXPORT3" è stata modificata in modo da consentire l'impiego di algoritmi di cifratura deboli nel portale per l'autenticazione. (cfr. sezione "problemi noti" nella versione 7.0.1).

Proxy

Proxy HTTP

Una volta attivata la scansione antivirus, il proxy http modificherà le queries che richiedono una compressione in modalità "deflate", per evitare tale compressione. Questa modalità di compressione difatti non consente di condurre una scansione antivirus affidabile.

ICAP

Riferimento assistenza: 14443

Il peso massimo dei file che possono essere ricevuti dal modulo ICAP in "response mode" è stato modificato, passa quindi da 2.5 KB a 4 KB per migliorare l'analisi di siti web che impiegano cookies di grandi dimensioni.

NS-BSD

PKI

Riferimento assistenza: 14573

I comandi di importazione/esportazione dei certificati sono ora dotati del nuovo parametro "format" i cui valori possono essere "pem" o "der" (ad esempio format=pem). I certificati possono quindi essere importati in questi due formati. I comandi interessati da questa modifica sono "CA GET", "CA CRL GET" e "CONFIG CERT ADD".

Nota: laddove mancasse il parametro "format", il formato impiegato sarà "der" per i comandi "CA GET" e "CA CRL GET" e "pem" per il comando "CONFIG CERT ADD".

SSL VPN

Supporto di OWA 2007 in modalità premium

Il VPN SSL di NETASQ consente di accedere ai server OWA 2007 in modalità premium.

Incremento del numero di server VPN SSL

Riferimento assistenza: 14705

Nei modelli F200 e superiori è stato aumentato il numero dei server web e "altri" configurabili.

- F25, F50, F60 : 64 http - 32 altri
- F200, F500 : 128 http - 64 altri
- F800, F1200, F2500 : 256 http - 128 altri
- F5500 : 512 http - 256 altri

Client SNMP

Supporto di più "community"

Riferimento assistenza: 14787

Qualora si impieghi il protocollo SNMP in v1 o v2, il campo "community" consentirà di inserire più nomi di comunità, separati con una virgola.

NETASQ REAL-TIME MONITOR

Allarmi: quarantena

Riferimento assistenza: 145254

Nella finestra degli allarmi del NETASQ REAL-TIME MONITOR è disponibile una nuova opzione premendo il tasto destro del mouse. La nuova funzione "quarantine source" consente di mettere in quarantena uno host sorgente per un dato periodo di tempo.

NETASQ UNIFIED MANAGER

Scripting: nuove macro

Sono stati aggiunti i seguenti parametri di scripting - %HA_PEER_SERIAL% che contiene il numero di serie dell'appliance passiva in un cluster e %HA-PEER_FIRMWARE% che contiene informazioni sulla versione del firmware del dispositivo passivo nel cluster.

Licenze: Reperimento licenze per dispositivi passivi

Il modulo che consente il reperimento automatico delle licenze per un dato gruppo di prodotti è stato modificato in modo da consentire lo scaricamento di licenze per i dispositivi passivi in un cluster. I file contenenti tali licenze possono essere impiegati poi in uno script.

7.0.2: Bug fixes

NS-BSD

RAID

Riferimento assistenza: 14657

L'impiego anomalo delle risorse della CPU in caso di accessi simultanei allo strumento di diagnosi RAID è stato corretto.

ASQ

Identificazione di evasioni %u nelle URL

L'identificazione di tentativi di evasione sui caratteri ASCII con codifica %u è stata modificata onde poter considerare solo quei caratteri con "valore inferiore a" (al contrario del precedente parametro "256").

Configurazione allarmi SSL

Riferimento assistenza: 14738

La finestra di configurazione per alcuni allarmi del plugin SSL consentiva di modificare l'azione (p.es. "pass" o "block") nonostante la configurazione manuale di tale azione non fosse consentita. La visualizzazione di tali impostazioni si limita ora al parametro "block".

Active Update

Aggiornamento Optenet

Riferimento assistenza: 14821

Il modulo è stato rivisto onde correggere un problema che non consentiva di aggiornare parzialmente la banca dati Optenet.

Aggiornamento Kaspersky: disattivazione durante aggiornamenti maggiori

Riferimento assistenza: 14741

In fase di aggiornamento del software dalla versione 6.3 a volte l'aggiornamento delle banche dati Kaspersky veniva disattivato. La procedura di aggiornamento è stata modificata per correggere tale errore.

Proxy

Filtri URL: categorie errate nei log

Riferimento assistenza: 14731

A volte, qualora una policy di filtraggio web contenesse una regola del tipo "any@<adresse IP >", la categoria indicata nei log era scorretta.

Filtri URL: blocchi eccessivi

Riferimento assistenza: 14689

A volte, qualora una policy di filtraggio web fosse stata assegnata ad un utente o ad un gruppo di utenti, gli utenti interessati potevano subire erroneamente blocchi eccessivi del loro accesso ai siti.

Antispam: impiego della cache DNS

Riferimento assistenza: 14450

Ripristinare una configurazione antispam che impiegava la cache DNS su modelli che non supportano tale funzioni cagionava talvolta un malfunzionamento del modulo antispam.

Antispam: file di configurazione corrotto

Riferimento assistenza: 14719

Correzione del potenziale crash del proxy qualora il file di configurazione delle blacklist DNS sia corrotto e contenga riferimenti a server inesistenti.

SSL VPN

Perfezionamento dell'elaborazione di URL complesse

Il modulo che rielabora le URL collegate, presenti all'interno dei siti, è stato perfezionato ed è ora in grado di modificare correttamente talune URL complesse.

Perfezionamento del supporto di javascript

Riferimento assistenza: 14661

Il modulo che rielabora gli script java nelle pagine web è stato perfezionato onde considerare anche i commenti presenti negli script.

Autenticazione

Modificare una password scaduta

Riferimento assistenza: 14637

Ora è possibile modificare la password nella pagina dell'autenticazione anche qualora la vecchia password sia scaduta..

Autenticazione Kerberos: campo "password" vuoto

Riferimento assistenza: 14693

Nella modalità di autenticazione Kerberos vengono ora accettati anche campi "password" vuoti.

NTP

Oggetti globali

Riferimento assistenza: 14735

Il modulo NTP consente di impiegare oggetti globali come server.

NETASQ UNIFIED MANAGER

Download di licenze con versione > v8

Riferimento assistenza: 14747

Il NETASQ UNIFIED MANAGER non considera più la licenza v8 come la versione più recente e scarica quindi le licenze in versioni superiori (v9 e superiori).

Eliminazione di allarmi non necessari

Riferimento assistenza: 14604

Diversi allarmi non necessari generati dal NETASQ UNIFIED MANAGER sono stati cancellati.

Filtri URL : controllo della coerenza

Riferimento assistenza: 14681

Diversi allarmi non necessari generati quando si impiegano oggetti dinamici sono stati cancellati.

Global Administration: ping

Riferimento assistenza: 14773

Questa funzione é stata modificata ed ora considera anche tutte le risposte ICMP generate dopo un ping per controllare la disponibilit  della host remoto.

Aggiornamento web: caratteri speciali

Riferimento assistenza: 14543

È stato perfezionato il supporto dei caratteri speciali presenti nel campo "password" dell'aggiornamento web.

7.0.3: Vulnerabilit  rimosse

ClamAV Antivirus

Correzione di diverse vulnerabilit  che potevano avere conseguenze serie come il denial of service (CVE-2007-6325, CVE-2007-6336, CVE-2007-6337, CVE-2008-0318, CVE-2008-0728). Il motore ClamAV é stato aggiornato alla versione 0.92.1. Nota: Dalla versione 6.2 in avanti, il server ClamAV operava senza alcun privilegio (utente *nobody*). Nella configurazione standard dei prodotti NETASQ é disattivato.

LDAP

Correzione di un possibile denial of service sul server LDAP, dovuto ad una query LDAP appositamente generata (CVE-2008-0658). Il modulo LDAP é stato aggiornato alla versione 2.3.41. Nota: Nella configurazione standard il modulo LDAP non é attivato.

PostgreSQL

PostgreSQL aggiornato alla versione 8.2.6 onde correggere diverse vulnerabilit  (CVE-2007-6600, CVE-2007-4772, CVE-2007-6067, CVE-2007-4769, CVE-2007-6601). Nota: La banca dati PostgreSQL fa parte del pacchetto di installazione sul modulo "Collector". Qualora si installasse il "Collector" nella versione 7.0.3, l'Administration Suite richiede la disinstallazione delle versioni precedenti prima di completare l'installazione della nuova versione. PostgreSQL non fornisce alcun aggiornamento automatico del motore, durante l'aggiornamento i dati vengono mantenuti.

7.0.3: Funzioni

NS-BSD

Script di configurazione standard (defaultconfig)

Il segnale acustico che indica l'avvio dello script di configurazione standard é stato modificato. Nelle versioni precedenti il segnale consisteva di sei toni consecutivi. Dalla versione 7.0.3 in avanti il segnale acustico é stato modificato e dotato di una nuova sequenza onde distinguere le diverse procedure:

1. vengono emessi 2 toni per indicare l'avvio della procedura
2. La sequenza di 2 toni si ripete al termine del controllo e del back-up dei dati
3. 4 toni vengono emessi al termine della procedura di configurazione standard
4. 1 tono aggiuntivo verr  emesso in caso di rebooting del dispositivo.

Script "getlicense" aggiunto

A questo script si accede esclusivamente nella modalit  operativa "console" e consente di reperire il file con la licenza dal sito NETASQ. Il comando "getlicense -h" consente di visualizzare i diversi parametri disponibili.

ASQ

HTTP: normalizzazione degli indirizzi URL

Abbiamo aggiunto una nuova analisi al plugin http per ostacolare eventuali tentativi di trafugamento dei dati. Ciò si realizza normalizzando gli URL prima di inserirli nelle firme contestuali. Indirizzi contenenti elementi quali la "self reference (./)" o la "directory traversal (../)" verranno tradotti dal plugin ASQ e l'indirizzo sarà normalizzato prima di essere analizzato. Ad esempio l'URL `/Folder/./Test/./index.html` diventerà `/Folder/index.html` in sede di analisi.
Nota : ASQ non modificherà i dati di rete.

Nuovo avviso protocollare

È stato creato un nuovo avviso: "**path with higher reference outside root directory**" (il percorso si riferisce ad una directory al di fuori della root). Questo avviso è stato inserito nella sezione "Protocol" nel contesto "http" (id 124). Tale avviso consente di identificare URL contenenti `"../index.html"` che presentano quindi collegamenti a file al di fuori del percorso dell'attuale directory. La configurazione standard legata a questo avviso è "block, major" in tutti i profili.

IPSec VPN

Catene di certificati della CA

Il modulo VPN IPSec può impiegare le informazioni fornite dalla "Certification Authority" (CA) e contenute nella directory LDAP, qualora sia stata attivata l'opzione "Trust internal PKI" (PKI interna affidabile). Nelle versioni precedenti potevano verificarsi errori qualora la directory LDAP contenesse più certificati (profili d'identità che includono l'attributo `cACertificate` nel campo DN). Dalla versione 7.0.3 in avanti, il modulo IPSec VPN carica tutti i CA rinvenuti nella directory ed accetta quindi tutti i certificati firmati anche qualora appartengano a catene di autorizzazioni.

Selezione dei campi d'identificazione nel certificato

Riferimento assistenza : 15330

Nella maggior parte dei casi, il modulo VPN IPSec impiega il campo "indirizzo e-mail" di un certificato per identificarne l'utente. Ciò nonostante alcune architetture possono richiedere l'impiego di un ulteriore campo nel certificato.

Questa funzione è disponibile impiegando una directory LDAP. Per utilizzarla, è necessario modificare la configurazione del file della policy IPSec VPN in uso (file 01 - 10). Nei campi `CertNID` (48 nella versione standard) e `LdapField` (indirizzo e-mail nella versione standard) vanno impostati i valori desiderati.

Esempio : file 01, sezione « Global »

```
[Global]
CertNID=458
LdapField=UID
```

Campi del certificato	CertNID	Commento
emailAddress	48	Indirizzo email (pkcs9)
mail	460	Indirizzo email (RC822)
UID	458	User ID (login)
CN	10	Nome comune
SN	100	Cognome
GN	99	Nome assegnato

Autenticazione

Catena gerarchica di CA ed autenticazione SSL

Impiegando l'autenticazione SSL, il modulo di autenticazione userà automaticamente la directory LDAP interna o esterna. Nelle versioni precedenti questa procedura poteva generare un errore, qualora la directory LDAP contenesse diversi CA (profili d'identità che includono l'attributo `cACertificate` nel campo DN). Dalla versione 7.0.3 in

avanti, il modulo the IPsec VPN carica tutti i CA presenti nella directory ed accetta quindi tutti i certificati firmati, anche inerenti a catene di autorizzazioni CA.

NETASQ UNIFIED MANAGER

Sincronizzazione della configurazione nella modalità "global administration"

Qualora la configurazione di due dispositivi installati in un cluster ad alta disponibilità (HA) venga modificata in modalità global administration, l'applicazione richiederà di sincronizzare le configurazioni.

NETASQ REAL-TIME MONITOR

Visualizzazione degli avvisi: id field

È stato aggiunto il campo *id* alla maschera di visualizzazione degli avvisi, per facilitare l'identificazione dei diversi allarmi. L'identificazione complete di un avviso implica quindi il contest e l'identifier (ad esempio contesto: http:url:client — id : 2).

7.0.3: Bug fixes

Antivirus

Rischio di "overflow" sui modelli F25-B, F50-B ed F50-C

Riferimento assistenza: 15336, 15339

Nelle scorse settimane l'enorme incremento del numero di firme antivirus contenute nella banca dati (+50% solo negli scorsi due mesi) ha originato l'eventualità di un overflow a medio termine su alcuni dispositivi prodotti nel 2004 e nel 2005: F25-B, F50-B, F50-C. Per evitare di incorrere in tale rischio, NETASQ e Kaspersky hanno dato vita ad una soluzione comune ed efficace a lungo termine.

Aggiornando i dispositivi F25-B, F50-B, F50-C (con numeri di serie che iniziano con F25-XB, F25-XC e F50-CC), che impiegano ClamAV si migra automaticamente al motore antivirus Kaspersky.

L'intera banca dati delle firme antivirus sarà disponibile su questi dispositivi, l'ottimizzazione consiste difatti in una selezione dinamica delle firme caricate in memoria.

Questo aggiornamento è gratuito. L'opzione Kaspersky sarà attivata fino al termine del contratto di manutenzione.

IPSec VPN

Disabilitato il campo per il debug VerifyCert

Riferimento assistenza: 15306

Nelle precedenti versioni il campo "VerifyCert" veniva impiegato per controllare il corretto funzionamento del firmware NETASQ. In alcuni casi tali controlli richiedevano difatti l'impiego di questo campo per il debug, ove la GUI inseriva un valore molto lungo. Per evitare tale problema questo campo non viene più considerato dalla configurazione.

Per i prodotti che impiegano tunnel IPsec con certificati, si raccomanda fortemente di verificare tali certificati (validità e catena gerarchica delle autorizzazioni) poiché attivando la modalità di debug, il tunnel non sarà più utilizzabile (il sistema emetterà il relativo avviso di errore).

ASQ

edonkey plugin

Riferimento assistenza: 13806

Correzione del plugin edonkey per prevenire un eventuale rischio di crash del modulo.

Trattamento dei pacchetti ICMP

Riferimento assistenza: 14975

La reazione del protocollo ICMP all'identificazione di pacchetti ICMP ECHO doppi è stata modificata. Qualora il pacchetto ICMP ECHO analizzato contenga la stessa ID di un pacchetto precedente però dati differenti, si genera l'allarme "ICMP ECHO data modified" (avviso protocollare, contesto icmp, id 109). Il comportamento del dispositivo dipende dall'azione configurata per questo allarme:

- Se l'azione è "block", il secondo pacchetto ICMP ECHO sarà bloccato
- Se l'azione è "pass", il secondo pacchetto ICMP ECHO verrà inoltrato e le informazioni sulla sessione saranno aggiornate

SSL plugin

Riferimento assistenza: 15117

Il plugin SSL è stato modificato per consentire il passaggio del protocollo TLS v1 dopo una negoziazione SSL v3. In precedenza alcune sincronizzazioni software condotte con ActiveSync venivano erroneamente bloccate.

SMTP plugin

Riferimento assistenza: 14585

Il traffico binario non viene più bloccato automaticamente all'interno di connessioni SMTP

Filtraggio

Opzione ASQ "ignora plugin"

La valutazione che consente di decidere se sia opportuno impiegare o meno un'analisi a livello applicativo (plugin) è stata modificata. Nelle versioni precedenti, l'attivazione di un plugin su un dato servizio (p.es. l'attivazione del plugin HTTP sul servizio HTTP) aveva la priorità rispetto all'opzione "non attivare il plugin", disponibile nella maschera avanzata del filtraggio (colonna "opzioni ASQ"). Dalla versione 7.0.3 in avanti, l'opzione "non attivare il plugin" ha la priorità sulla colonna "servizio".

NS-BSD

Organizzazione dei dati di aggiornamento della banca dati degli URL

Lo stoccaggio delle banche dati di URL (NETASQ ed Optenet) è stato riorganizzato onde migliorare la stabilità degli aggiornamenti automatici. Nota : Alcuni file sono stati spostati. Di conseguenza con la versione 7.0.3 non sarà possibile ripristinare le banche dati di URL da un backup effettuato con una versione precedente.

Invio di pacchetti ICMP Redirect

L'avviso "ICMP redirection" (id 22) veniva reiterato più volte qualora l'azione rispettiva fosse stata impostata su "block". Per evitare inutili allarmi, il comportamento del firewall è stato modificato, in caso di "block" i pacchetti ICMP redirect non vengono più inviati.

QoS

Configurazione asimmetrica

Il modulo QoS consente di configurare all'interno di una singola regola diversi limiti o quantitativi di banda da riservare in base alla direzione del flusso dei dati (in ingresso o in uscita). Qualora tali parametri venissero definiti solo per il traffico in uscita, lo stesso limite veniva applicato anche al traffico in entrata. Questo problema è stato risolto.

Proxy

Miglioramento della performance in caso di elevato traffico

Riferimento assistenza: 13252, 14318, 15084

Le operazioni del proxy sono state ottimizzate onde migliorarne la performance in caso di traffico elevato.

HTTP Proxy

Riferimento assistenza: 15200

Il proxy HTTP accetta la cifratura "pack200-gzip".

ICAP

Chiusura del collegamento

Riferimento assistenza: 15087

Abbiamo modificato il comportamento del proxy onde forzare la chiusura dei collegamenti tra il client host ed il server ICAP al termine della connessione con il web server.

OPTENET filtering

Riferimento assistenza: 15382

L'opzione di licenza che consente l'aggiornamento delle banche dati Optenet non dipende più dall'aggiornamento standard della banca dati URL. Questa modifica consente di aggiornare le banche dati Optenet fino all'esaurimento dell'opzione anche qualora il contratto di servizio sull'apparecchio sia scaduto.

SMTP Proxy

Riferimento assistenza: 15349

La gestione degli eventi che danno luogo all'errore "552 Data size exceeded" (superamento della grandezza consentita) è stata modificata. Il proxy invia la risposta del server al termine della richiesta del client.

Amministrazione del proxy

Riferimento assistenza: 15037

La configurazione del proxy può essere cambiata dagli utenti che hanno il diritto di lettura / scrittura "base, url, modify".

SSL VPN

Riscrittura dei collegamenti ipertestuali

Riferimento assistenza: 15004, 15195, 15428

Il motore di riscrittura dei collegamenti ipertestuali è stato migliorato, in special modo per la riscrittura di script java.

NETASQ UNIFIED MANAGER

Licenza

Le licenze possono essere aggiornate anche dopo lo scadere delle stesse (informazione contenuta nella sezione DATA, nel campo "license validity").

Modifica dei percorsi statici

Riferimento assistenza: 14793

Qualora il routing statico impieghi oggetti non più esistenti, l'amministratore di sistema ne viene informato e tali percorsi non vengono attivati.

La modalità Global Administration

Riferimento assistenza: 14773

Il ping per verificare la connettività di rete é stato modificato onde considerare tutti i tipi di risposta.

Backup di sistema

L'attività di backup di una partizione risultava a volte non selezionabile su modelli che la consentivano. Questo errore é stato corretto.

NETASQ REAL-TIME MONITOR

Allarmi

Diversi perfezionamenti della stabilità della finestra degli allarmi per evitare la chiusura dell'applicazione.

NETASQ EVENT REPORTER

Debug

Riferimento assistenza: 14782

I file per il debug sono raggruppati nella directory "C:\Documents and Settings\All Users\Application Data\AS\7.0\".

Autoreport

Supporto della data in formato italiano.

7.0.3: Problemi noti

Autenticazione ed Active Directory

Qualora il nome di un oggetto sia identico al dominio Active Directory, gli elenchi degli utenti non verranno caricati correttamente.

NS-BSD

Backup — Ripristino

I gruppi di URL (NETASQ ed Optenet) di cui é stato fatto un back up nelle versioni precedenti non possono essere ripristinati nella versione 7.0.3 poiché qui i file relativi sono stati spostati.

7.0.3.1 : Vulnerabilità rimosse

Antivirus ClamAV

Correzione di diverse vulnerabilità che potevano dar luogo persino a denial of service (CVE-2008-1100, CVE-2008-0314, CVE-.2008-1387, CVE-2008-1833).

Nota: Dalla versione 6.2 in poi, il server ClamAV operava senza alcun privilegio (utente *nobody*). Nella configurazione standard dei prodotti NETASQ é disabilitato.

7.0.3.1 : Funzioni

ClamAV Antivirus

Ottimizzazione dell'impiego del disco durante l'aggiornamento della banca dati antivirus.

7.0.3.1 : Bug fixes

NS-BSD

Supporto USB per il dispositivo U6000

Aggiornamento del sistema onde consentire l'impiego di una porta USB su U6000.

Rimozione del link simbolico ad una directory contenente log

Riferimento assistenza: 15685

Se si rinviene un link simbolico che punta alla directory "log" all'interno della cartella ConfigFiles, questo viene rimosso durante l'aggiornamento del sistema operativo. La presenza di tale link potrebbe difatti avviare il processo di backup della directory di log.

7.0.4: Caratteristiche

ASQ

Plugin RTP — RTCP

Riferimento assistenza: 15798

Questi plugin sono impiegati per controllare i pacchetti RTCP in conformità con RFC 3550. Alcuni parametri, possono essere impiegati durante la configurazione per autorizzare specifici codici RTP e operazioni RTCP.

Per evitare qualsiasi tipo di rischio durante il processo di aggiornamento, i file di configurazione di ASQ non vengono modificati. L' interfaccia grafica non mostra quindi i parametri RTP – RTCP. Nella fase di attivazione dei plugin bisogna impostare manualmente questi parametri secondo i seguenti valori consigliati da NETASQ:

- "AllowCodec": specifica i codici autorizzati per mezzo di set di valori separati da virgole (cfr. RFC 3551).
Nota: Il valore raccomandato per questo parametro è "0-18,25,26,28,31-34,96-127".
- "AllowOp": abilita l'autorizzazione di operazioni aggiuntive. Le operazioni permesse di default sono: FIR(192) - NACK(193) - SR(200) - RR(201) - SDES(202) - BYE(203) - RTPFB(205) - XR(207).

I valori dell'operazione sono tratti da RFC 3550.

Nota: Il valore consigliato per questo parametro è "".

- "DenyOp": consente di proibire determinate operazioni. La differenza tra un'operazione bloccata ed una consentita risiede nelle notifiche di errore mostrate: un pacchetto che contiene operazioni non autorizzate produrrà l'allarme "operazione non supportata", un pacchetto con operazioni proibite "operazione bloccata".

Nota: Come raccomandato da RFC 3550, il valore standard è "204" (APP operation).

Le notifiche di errore associate con i plugin RTP — RTCP in ASQ sono:

- "Invalid RTP Version": il valore dei primi due bit del pacchetto RTP non è "10".
- "Invalid RTP data type": il campo che contiene informazioni sul tipo di file (PacketType) presenta un parametro non consentito da "Codec allowed".
- "Invalid RTP protocol (packet too short)": il pacchetto ricevuto è troppo corto per poter contenere un header RTP completo.
- "Invalid RTCP version": il valore dei primi due bit del pacchetto RTCP non è "10".
- "Invalid RTCP data type (unknown)": il campo che contiene informazioni sul tipo di file (PacketType) presenta un parametro non consentito da "Operation allowed".
- "Invalid RTCP data type (denied)": il campo che contiene informazioni sul tipo di file (PacketType) presenta un parametro espressamente proibito in "Operation prohibited".
- "Invalid RTCP protocol (packet too short)": il pacchetto ricevuto è troppo corto per poter contenere un header RTCP completo.

Pseudo-conessioni UDP

Perfezionamento della gestione a senso unico dei dati UDP

L'applicazione REAL-TIME MONITOR di NETASQ mostra informazioni sulle sessioni UDP unidirezionali (richieste DNS ed NTP senza risposta, traffico RTP).

Routing avanzato

Controllo della disponibilità di una route

Riferimento assistenza : 15580

La disponibilità di un dato percorso può essere controllata testando l'accessibilità di un gruppo di host attraverso un router. Per effettuare tale controllo, si possono associare un host o un gruppo di host ad un dato percorso nella finestra "Network -> Routing" della scheda "Advanced". Se non ci sono host specificati, il controllo della disponibilità verrà effettuato sull'indirizzo IP del router (come nella versione precedente).

Nota: Si consiglia di restringere il numero di gruppi controllati a 3.

Parametri di controllo

Il valore standard del campo "Wait" per il controllo di un percorso è stato diminuito da 10 a 5 secondi. Questo parametro definisce il tempo di attesa tra due ping impiegati per controllare un dato percorso. Dal momento che un percorso si può verificare impiegando molteplici indirizzi IP, il tempo di attesa è stato ridotto in modo che il numero di test condotti sui vari host non superi la frequenza stessa dei test.

NETASQ SEISMO

È stato modificato il comportamento della licenza SEISMO che si avvicina alla scadenza. Quando scade l'opzione di aggiornamento del database delle vulnerabilità, non verranno più fornite le informazioni SEISMO, bensì il NETASQ REAL-TIME MONITOR visualizzerà logs, notifiche SNMP ed email.

Nota: L'opzione di aggiornamento della banca dati delle vulnerabilità può essere riattivata scaricando una licenza valida.

Sistema

Autenticazione

Il portale di autenticazione è ora disponibile anche in polacco.

ClamAV

Il motore ClamAV è stato aggiornato alla versione 0.93.1

Nota: le vulnerabilità ClamAV risolte aggiornando il motore alla versione 0.93.1, erano già state risolte nella versione 7.0.3.1 del motore NETASQ.

NETASQ UNIFIED MANAGER — Tempi di chiusura della connessione

Riferimento assistenza: 15323

Il valore minimo standard del parametro "Closed connection timeout" nell'applicazione NETASQ UNIFIED MANAGER è stato ridotto da 10 a 2 secondi. Questo valore indica i secondi in cui la connessione verrà mantenuta dopo la ricezione di un pacchetto di chiusura connessione.

Nota: Il valore di 2 secondi è consigliato solo per reti con molto traffico.

NETASQ REAL-TIME MONITOR

Le finestre di log presentano ora un maggior numero di informazioni, con l'aggiunta delle seguenti colonne:

- Schermata traffico: indirizzi IP di origine e di destinazione (mascherati di default), utente e interfaccia di origine.
- Schermata filtro: indirizzi IP di origine e di destinazione (mascherati di default), utente e interfaccia di origine.
- Schermata VPN: indirizzi IP di origine e di destinazione (mascherati di default).

Nota: Un clic col tasto destro sui titoli di una data colonna consente di visualizzare le colonne nascoste di default.

7.0.4: Bug fixes

ASQ

Overflow della queue TCP

Riferimento assistenza: 15747

Il meccanismo che protegge da denials of service TCP si apre ora in una finestra di maggiori dimensioni.

Routing

Il motore ASQ non controlla più eventuali percorsi alternativi qualora il "route load balancing" sia disabilitato.

Proxy

HTTP — Traffico audio

Riferimento assistenza: 15406

Il proxy HTTP consente la trasmissione in tempo reale del traffico audio.

HTTP — Bypass antivirus

Riferimento assistenza: 15880

La funzione “Bypass antivirus” è stata aggiunta al controllo dei contenuti in tempo reale. Nella configurazione standard i seguenti caratteri MIME non saranno sottoposti ad una scansione antivirus non necessaria:

- video/*
- audio/*
- application/sdp
- application/vnd.ms.wms-hdr.asfv1
- application/x-mms-framed

SSL VPN

Compatibilità OWA 2003

Riferimento assistenza: 15648

La compatibilità con OWA 2003 è stata perfezionata. La riscrittura di query HTTP POST è stata corretta.

Lista bianca di URL

Riferimento assistenza: 15665

L'impiego del carattere '*' per riscrivere indirizzi web funziona correttamente. La lista bianca degli URL contiene link che non devono essere riscritti dai componenti SSL VPN. Quando si usa il carattere "*", i componenti SSL VPN terranno il seguente comportamento:

- I link ai siti esterni non verranno riscritti
- I link ai siti interni (protetti da SSL VPN) verranno riscritti per imporre la deviazione a SSL VPN.

Autenticazione

Compatibilità Radius

Riferimento assistenza: 14369

La compatibilità RADIUS è stata migliorata. L'attributo NAS-ID (numero di serie dell'appliance) è stato aggiunto alle query RADIUS per garantire la compatibilità con i prodotti Middleware 3.0 di VASCO.

Sistema

Alta affidabilità

Riferimento assistenza: 15677

Quando la funzione “ActiveUpdate” è attivata, l'aggiornamento della licenza Kaspersky sull'appliance attiva verrà correttamente copiato sulla appliance passiva di un cluster ad alta affidabilità.

SNMP

Riferimento assistenza: 14312

La visualizzazione della stato dell'Interfaccia ethernet (ifOperStatus) è stata corretta.

Backup / Ripristino

Nel ripristino di un backup effettuato su appliance con versione inferiore alla 7.0.3, i gruppi di URL filtrati non vengono più presi in considerazione. Poiché la destinazione dell'archiviazione dei gruppi di URL filtrati è stata modificata nella versione 7.0.3, i dati verrebbero duplicati in caso di ripristino dei gruppi da un backup generato con una precedente versione.

NTP

È stato corretto un errore comparso occasionalmente durante la cancellazione del server NTP.

NETASQ UNIFIED MANAGER

Importazione / Esportazione

Riferimento assistenza: 15893

I numeri di serie delle appliance sono stati aggiunti all'elenco dei dispositivi gestito con la funzione "Importing / Exporting firewall file". Il campo "Serial number" si trova subito dopo il campo "Password".

Nota: Per evitare un'alterazione della visualizzazione (colonne sfasate) dei dati dopo l'importazione di un file da una versione precedente alla 7.0.4, si consiglia di modificare il file esportato (formato CSV) aggiungendo una colonna dopo la colonna "Password".

Modulo di scripting

Riferimento assistenza: 15750

È possibile trasferire più file con un singolo comando.

Esempio: Importare un certificato X509

```
Config cert add name=usercert type=privkey format=pem $FROM_TEXT_FILE("D:\Cert\user_cert.pem", "D:\Cert\user_key.pem")
```

Nota: Seguire l'ordine dei file (file contenente il certificato seguito dal file contenente la chiave privata).

Informazioni sulla partizione di backup

Le informazioni riguardanti la partizione di backup vengono visualizzate correttamente a seguito di un'operazione di partizione di backup andata a buon fine.

NETASQ REAL-TIME MONITOR

Informazione "IP"

Riferimento assistenza: 15340

La colonna "IP" è stata aggiunta alle finestre "Alarm" (nascosta nella configurazione standard) e "Logs -> Traffic" (visibile nella configurazione standard).

Organizzazione delle connessioni

Nella finestra "Hosts", la selezione delle connessioni in base al volume di dati (spediti e ricevuti) è stata migliorata. Alcune connessioni aperte dinamicamente dai plugin vengono ora visualizzate correttamente.

7.0.5: Vulnerabilità risolte

LDAP

Correzione di una falla che avrebbe potenzialmente generato un denial of service (CVE-2008-2952).

IPSec VPN

Correzione di una falla relativa all'uso della memoria durante il trattamento di proposte di parametrizzazione IPSec non corrette.

7.0.5: Caratteristiche

ASQ

Sequenzializzazione dei pacchetti IP

Riferimento assistenza: 12037

È stata perfezionata la gestione dei frammenti “erranti” di pacchetti IP da parte del motore ASQ. La gestione di pacchetti frammentati viene inizializzata non appena ASQ riceve un qualsiasi frammento all'interno di una sequenza. Questa miglioria non ha alcun impatto sull'analisi protocollare condotta dai dispositivi NETASQ .

Rimozione dei log sul traffico bloccato

Riferimento assistenza: 15669

Il modulo di registrazione dei log è stato perfezionato per dare maggior priorità ad eventi relativi al traffico autorizzato qualora la coda dei log raggiunga il livello di saturazione (troppi eventi da gestire). È quindi possibile configurare una percentuale di saturazione della coda, che, una volta raggiunta, non consentirà di inserire nei log informazioni su eventi legati al traffico bloccato. Tale opzione consente di preservare il sistema da contro gravi saturazioni ed è disponibile sia sui log di filtro sia sui log relativi agli allarmi.

7.0.5: Bug fixes

Sistema

Antivirus ClamAV

Il motore antivirus ClamAV è stato aggiornato alla versione 0.93.3.

La gestione delle banche dati di signature è stata migliorata in modo da ottimizzare l'impiego della memoria disponibile nei prodotti NETASQ. I file vengono letti direttamente dagli archivi compressi, evitando quindi l'archiviazione di file decompressi con il conseguente risparmio di in termini di capacità di memoria.

Nota: Il formato compresso sarà applicato a partire dal prossimo Active Update che ha luogo, per le configurazioni standard, subito dopo l'aggiornamento del software.

Kaspersky Antivirus

Il numero di file scaricabili attraverso il modulo dell'Active Update è stato incrementato. Ciò consente ai dispositivi NETASQ di accettare una banca dati di signature dalle dimensioni più ampie per il motore antivirus Kaspersky.

ARP Cache e banca dati degli oggetti

Riferimento assistenza: 12827

Il comando per la configurazione contenente indirizzi MAC viene ora trattato correttamente.

ASQ

Configurazione del plugin RTP — RTCP

Il motore ASQ è stato modificato in modo da impiegare i dati sulla configurazione standard presenti nel plugin RTP-RTCP, tale configurazione sarà applicata qualora non sia presente alcuna altra informazione nel file di configurazione.

7.0.5: Problemi noti

Backup / Ripristino

I backup di gruppi di URL (moduli per il filtraggio web NETASQ e Optenet) creati nelle versioni inferiori alla 7.0.3 non vengono ripristinati correttamente nella versione 7.0.3, bensì nella cartella errata.

Reti — VLAN

Le VLAN collegate ad un'interfaccia Ethernet disabilitata non funzionano correttamente se l'interfaccia master è stata configurata con DHCP. Tale problema si risolve configurando un indirizzo IP statico per l'interfaccia master.

Autenticazione

Creando un oggetto "host" che abbia lo stesso nome di un dominio Windows, si compromette l'integrazione con la componente Microsoft Active Directory. In questo caso infatti NETASQ non può recuperare l'elenco degli utenti.

7.0.6: Caratteristiche

ASQ

Plugin SSL

L'analisi dei protocolli TLS 1.1 e TLS 1.2 è ora integrata nel plugin SSL.

Plugin DNS

Due nuovi allarmi DNS sono stati aggiunti per completare e meglio specificare i risultati delle analisi condotte:

- **"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.

NAT

È consentita la selezione casuale dei numeri delle porte per le regole di reindirizzamento su una specifica porta.

Sistema

Autenticazione

Riferimento assistenza: 16771

Si possono condurre ricerche sui certificati presenti in una directory LDAP impiegando campi quali l'indirizzo e-mail, CN o UID. Nelle versioni precedenti si poteva utilizzare solo il campo inerente all'indirizzo email.

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

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

Inoltre, i dispositivi NETASQ ora accettano i certificati X.509 che contengano nel titolo campi DC (domainComponent).

7.0.6: 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).

Proxies

Miglioramenti delle richieste ICAP-REQMOD

Riferimento assistenza: 15836

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

Stabilità del proxy POP3

Riferimento assistenza: 16509

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

Antivirus: banca dati Kaspersky

Il pacchetto scaricato automaticamente con l'Active Update è stato modificato. Al posto del pacchetto "Kaspersky Embedded", il modulo scaricherà il pacchetto standard.

Nota: I modelli F25, F50 e F60 continueranno ad impiegare il pacchetto "Kaspersky Embedded".

System

Dimensione del token SPNEGO:

Riferimento assistenza: 16679

La dimensione del buffer di lettura è stata aumentata per supportare i token sovradimensionati. Il numero massimo di righe è passato da 3 a 20 KB.

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.

Gestione del servizio "subversion"

Riferimento assistenza: 16496

Corretto l'errore che non consentiva di assegnare i servizi di 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

Risoluzione DNS

Riferimento assistenza: 16669

Corretto l'errore di risoluzione DNS su oggetti dinamici causato in alcuni casi da ritardi delle risposte del server.

Inizializzazione crittografata del syslog

Riferimento assistenza: 17194

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

Informazioni sull'antivirus Kaspersky

Le informazioni riguardanti l'antivirus Kaspersky sono visualizzate con l'apposito comando solo sulle appliance dotate della relativa licenza.

Stabilità dei daemons

Corretti i daemons che si riavviano dopo modifiche alla data.

Alta disponibilità (HA)

Scambio improvviso durante la sincronizzazione

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

7.0.6: Vulnerabilità risolte

ClamAV

Il modulo ClamAV è stato aggiornato per correggere due vulnerabilità :

- buffer overflow (CVE 2008-5050) che in che in alcuni contesti può causare un denial of service sull'applicazione o sull'esecuzione del codice.
- JPEG crafted (Secunia Advisory SA32926) che, in alcuni contesti, potevano cagionare un denial of service dell'applicazione .

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

7.0.6: Problemi noti

Reti — VLAN

L'assegnazione di una VLAN ad un'interfaccia Ethernet disabilitata non funziona correttamente se l'interfaccia madre è stata configurata con DHCP. Per aggirare il problema è sufficiente specificare un indirizzo IP statico per l'interfaccia madre.

Autenticazione

Quando si crea un host con lo stesso nome del dominio dell'Active Directory, non è possibile recuperare correttamente la lista di utenti.

Velocità dell'interfaccia seriale

Il messaggio di sistema "more tty-level Buffer Overflow" compare occasionalmente sulla console dei prodotti U1100, U1500 e U6000 quando i caratteri vengono inviati più velocemente di quanto l'hardware li possa leggere.

7.0.6.1: Bug fixes

Antivirus

Scambio improvviso del motore antivirus

Riferimento assistenza: 17434

Corretto il passaggio inatteso del motore antivirus da ClamAV a Kaspersky. Questo scambio, inerente ai dispositivi F25, F50, F60 e F200 aveva luogo in seguito all'aggiornamento alla versione 7.0.6.

Sistema

Server PPTP

Riferimento assistenza: 16937

Risolti i problemi legati alla pubblicazione ARP delle connessioni PPTP con un ampio numero di interfacce.

Autenticazione KERBEROS

Riferimento assistenza: 15878

Le password KERBEROS ora possono contenere i caratteri speciali Latin-1.

7.0.6.2: Bug fixes

Interfacce di rete

Limiti VLAN ed MTU

Riferimento assistenza: 17465

Ora é possibile impostare un valore MTU fino a 1500 bytes per una VLAN configurata su un prodotto della serie U. In precedenza, mentre il valore MTU per un'interfaccia fisica non poteva superare i 1500 byte, le VLAN associatevi non potevano avere un valore MTU superiore ai 1496 bytes.

Funzioni della versione 7.0.7

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.

7.0.7: Bug fixes

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.

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.

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).

7.0.8: Vulnerabilità risolte

ClamAV

Il motore antivirus ClamAV é 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.

7.0.8: Bug fixes

Interfaccia di rete

U6000: Inizializzazione dell'interfaccia EM

Riferimento assistenza: 18410

Corretto l'errore di inizializzazione dell'interfaccia EM durante un switchover in alta affidabilità (HA).

ASQ

Plugin SSL

Riferimento assistenza: 17832

Corretto il messaggio "Invalid SSL packet (TLSv1)" che si presentava prematuramente.

Sistema

Syslog: trasferimento cifrato dei log

Riferimento assistenza: 18270

Qualora i log venissero trasferiti a due syslog server, venivano cifrati solo i dati destinati al primo server. Ora i dati vengono cifrati sempre, indipendentemente dal numero di syslog server a cui sono indirizzati.

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.

Pacchetti IKE_FRAG con formato inadeguato

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

Alta disponibilità

Eliminazione connessioni TCP switchate

Riferimento assistenza: 18094

L'anomalia concernente la cancellazione delle connessioni TCP switchate è stata corretta.

Stabilità durante il switchover

Il modulo di alta disponibilità (HA) è stato modificato onde migliorarne la stabilità durante il switchover.

Active Update

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.

7.0.9 : Vulnerabilità risolte

IPSEC VPN

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

7.0.9 : Bug fixes

Motore ASQ

Tabella hosts

Riferimento assistenza: 18869

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

Autenticazione

Signature degli applet sul portale

Riferimento assistenza : 18297

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

7.0.9 : Problemi noti

Interfacce di rete

VLAN 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.

Systema

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.