

Έργο: ΥπΕΠΘ - Τεχνικός Σύμβουλος 2007

**Υποέργο 17: «Υποστήριξη Συστημάτων Τεχνικής Στήριξης Σχολικών
Εργαστηρίων»**

Πακέτο Εργασίας 1

**«Ενίσχυση της λειτουργίας της κεντρικής υπηρεσίας του ΥπΕΠΘ για την Τεχνική
Στήριξη των ΣΕΠ»**

Τεχνική Αναφορά με τίτλο

«Οδηγίες υποστήριξης του Microsoft ISA Server 2000»

Έκδοση: 1.0

Οκτώβριος 2007

Σύνταξη:

Τομέας Εκπαιδευτικής Τεχνολογίας

Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών

ΥΠΟΥΡΓΕΙΟ ΕΘΝΙΚΗΣ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ

Περιεχόμενα

<u>1 Εισαγωγή.....</u>	<u>3</u>
<u>2 Γενική Υποστήριξη.....</u>	<u>3</u>
<u>2.1 Event Viewer.....</u>	<u>3</u>
<u>2.2 Ενημέρωση με νέες εκδόσεις.....</u>	<u>4</u>
<u>2.3 Services.....</u>	<u>4</u>
<u>2.4 Παρακολούθηση λειτουργίας.....</u>	<u>5</u>
<u>2.4.1 Log Files.....</u>	<u>5</u>
<u>2.4.2 Κονσόλα ISA Management.....</u>	<u>5</u>
<u>2.4.3 Αναφορές.....</u>	<u>7</u>
<u>2.4.4 Παρακολούθηση απόδοσης.....</u>	<u>9</u>
<u>2.5 Κοινά Προβλήματα.....</u>	<u>9</u>
<u>2.5.1 Οι σταθμοί εργασίας δε μπορούν να προσπελάσουν FTP sites μέσω του ISA Server 2000.....</u>	<u>9</u>
<u>3 Βιβλιογραφία.....</u>	<u>10</u>

1 Εισαγωγή

Στην παρούσα τεχνική αναφορά προτείνονται διαδικασίες υποστήριξης του λογισμικού ISA Server 2000 ως εφαρμογής proxy των σχολικών εργαστηρίων. Η τεχνική αναφορά αποτελεί μέρος του παραδοτέου του Πακέτου Εργασίας 1 «Ενίσχυση της λειτουργίας της κεντρικής υπηρεσίας του ΥπεΠΘ για την Τεχνική Στήριξη των ΣΕΠ», του Υποέργου 17 «Υποστήριξη Συστημάτων Τεχνικής Στήριξης Σχολικών Εργαστηρίων» του «Τεχνικού Συμβούλου ΥπεΠΘ 2007».

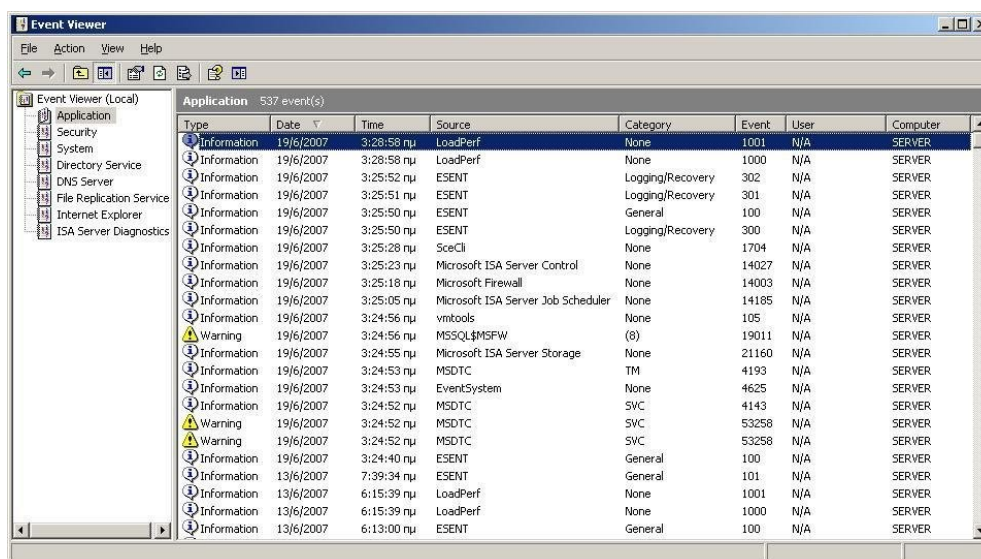
2 Γενική Υποστήριξη

2.1 Event Viewer

Το Λειτουργικό Σύστημα και οι εφαρμογές του καταγράφουν τα συμβάντα (events) της επιτυχούς ή μη εκκίνησης και ολοκλήρωσης διαφόρων διαδικασιών σε αρχείο καταγραφής. Ο διαχειριστής του συστήματος έχει πρόσβαση σε πληροφορίες των συμβάντων μέσω του εργαλείου Προβολής Συμβάντων (Event Viewer), οι οποίες περιλαμβάνουν:

- τον τύπο του συμβάντος (Information, Warning, Error)
- την ημερομηνία και την ώρα
- την πηγή του συμβάντος (στοιχείο του Λειτουργικού Συστήματος ή συγκεκριμένη εφαρμογή)
- την κατηγορία
- τον κωδικό αριθμό του
- το χρήστη που σχετίζεται με τη δημιουργία του συμβάντος
- τον υπολογιστή στον οποίο παρουσιάστηκε το συμβάν.

Τα συμβάντα του ISA Server 2000 καταγράφονται στο φάκελο συμβάντων Application.



Στον Event Viewer μπορούμε να ταξινομήσουμε τα συμβάντα χρονολογικά από την επικεφαλίδα της στήλης Date ή να ομαδοποιήσουμε τα συμβάντα σύμφωνα με τα περιεχόμενα των υπόλοιπων στηλών.

Κάνοντας διπλό κλικ σε ένα συμβάν βλέπουμε περισσότερες πληροφορίες για αυτό, που επεξηγούν την αιτία του προβλήματος. Για τις μεθόδους αντιμετώπισής του πρέπει να γίνει αναζήτηση στον κόμβο της Microsoft ή ακόμα και στο Διαδίκτυο για το συγκεκριμένο κωδικό (event id).

2.2 Ενημέρωση με νέες εκδόσεις

Η ενημέρωση του ISA Server 2000 με νέες εκδόσεις και διορθώσεις, πραγματοποιείται με εγκατάσταση των Service Packs και των patches από το site της Microsoft. Είναι απαραίτητο να είναι εγκατεστημένο το τελευταίο κάθε φορά Service Pack, το οποίο είναι διαθέσιμο μέσω του url "[How to obtain the latest Internet Security and Acceleration Server 2000 service pack](#)".

Καθώς ο ISA Server 2000 δεν υποστηρίζεται από το Microsoft Baseline Security Analyzer, η Microsoft προτείνει τον έλεγχο μέσω του ελεύθερου εργαλείου "[Shavlik NetChk Limited](#)".

Κατά τη στιγμή συγγραφής της αναφοράς δύο μόνο ενημερώσεις υπάρχουν για τον ISA Server 2000 SP2:

- η [MS04-039: Ένα θέμα ευπάθειας στον ISA Server 2000 και τον Proxy Server 2.0 θα μπορούσε να επιτρέψει την πλαστογράφιση περιεχομένου Internet](#) και
- η [MS05-034: Αθροιστική ενημερωμένη έκδοση ασφαλείας για τον Internet Security and Acceleration \(ISA\) Server 2000](#).

Παρόλο που η δεύτερη ενημέρωση είναι αθροιστική πρέπει να περάσουν και οι δύο στον εξυπηρετητή με setup αρχεία που παρέχονται από τα ανωτέρω άρθρα.

2.3 Services

Τα Services που τρέχουν στον ISA Server 2000 ανάλογα με τις ρυθμίσεις εγκατάστασής του είναι τα ακόλουθα:

- Microsoft Web Proxy
- Microsoft Scheduled Cache Content Download
- Microsoft ISA Server Control
- ISA Server Packet Filter Extension Driver
- Microsoft H.323 Gatekeeper

Αυτά τα Services πρέπει να είναι σε κατάσταση *Started* και με τύπο εκκίνησης *Automatic*, όταν τα ελέγχουμε μέσα από την κονσόλα Computer Management και στο μονοπάτι Services and Applications/Services.

2.4 Παρακολούθηση λειτουργίας

Η λειτουργία του ISA Server 2000 παρακολουθείται με τους ακόλουθους τρόπους:

1. Ενεργοποίηση log files και έλεγχος των περιεχομένων τους. Συνίσταται για την αντιμετώπιση συγκεκριμένων προβλημάτων και όχι για τη μαζική εξαγωγή στατιστικών αποτελεσμάτων.
2. Μέσω πληροφοριών και αναφορών από την κονσόλα ISA Management.
3. Με αναφορές (Reports).

2.4.1 Log Files

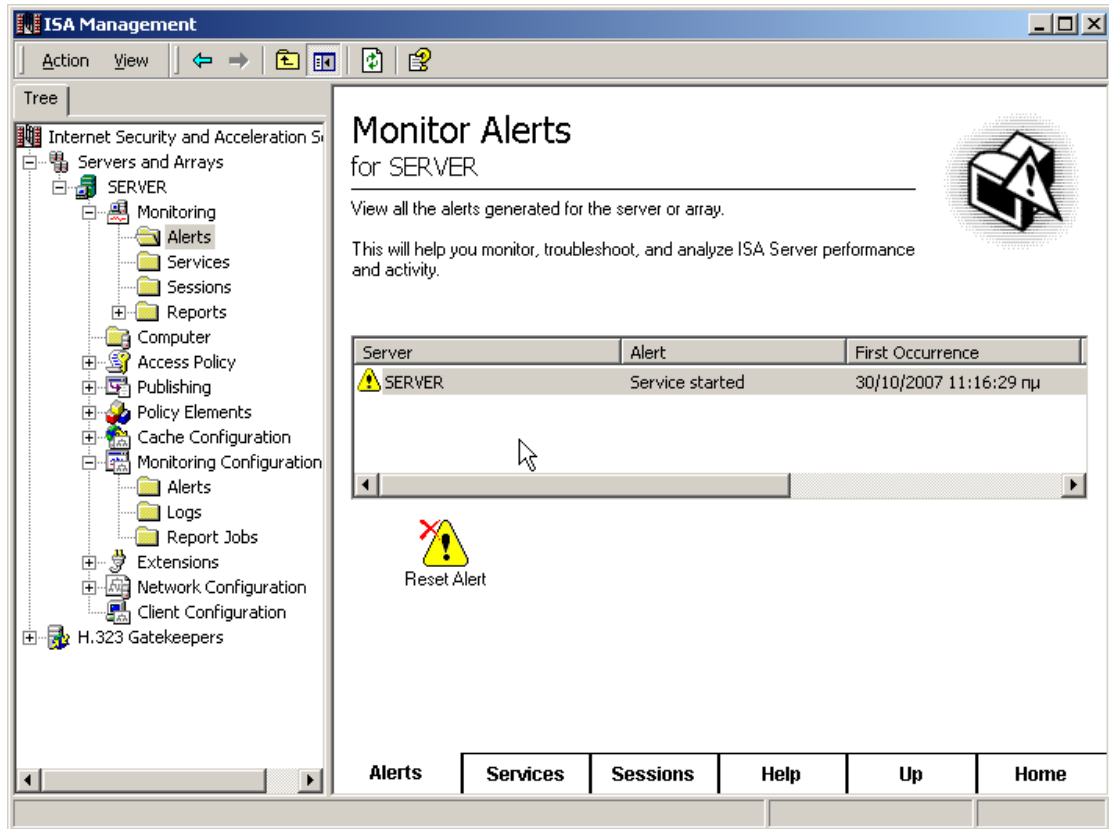
Η καταγραφή των λειτουργιών του ISA Server 2000 μπορεί να πραγματοποιείται σε Βάση Δεδομένων ή σε αρχείο. Για τις ανάγκες υποστήριξης των σχολικών εργαστηρίων η καταγραφή σε αρχείο κρίνεται περισσότερο κατάλληλη.

Η καταγραφή των σε log files ενεργοποιείται μέσω του ISA Management, όπου:

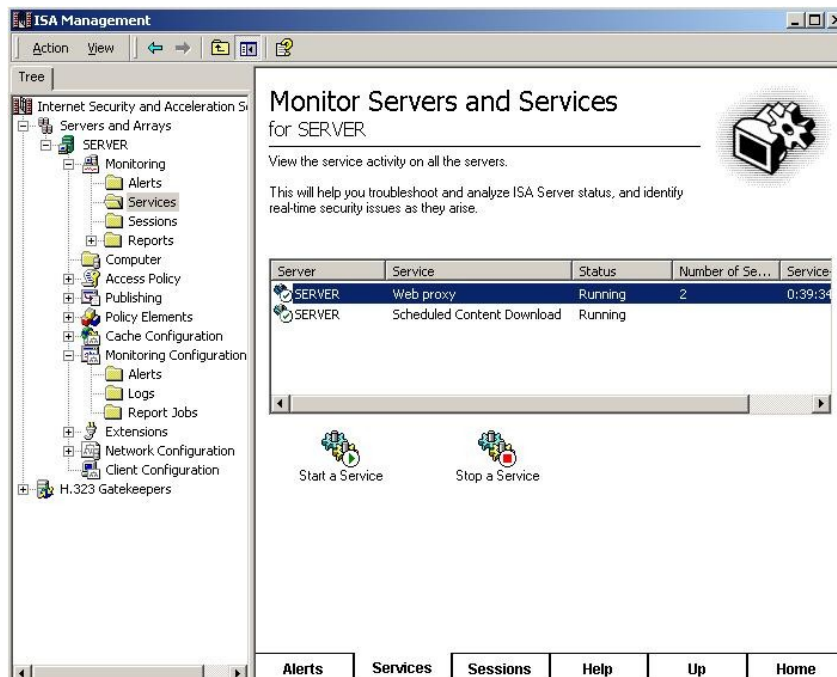
1. Στο μονοπάτι Servers and Arrays/SERVER/Monitoring Configuration επιλέγουμε Logs.
2. Στο Component ISA Server Web Proxy Service με δεξί κουμπί του ποντικιού επιλέγουμε Properties.
3. Στην καρτέλα Log επιλέγουμε File.
4. Στο Format επιλέγουμε τύπο αρχείου (W3C extended log file format).
5. Στην επιλογή Create New File επιλέγουμε την περίοδο δημιουργίας νέων αρχείων (Daily).
6. Επιλέγουμε Options.
7. Ενεργοποιούμε τη συμπίεση αρχείων και τη ρύθμιση Limit number of log files και επιλέγουμε το μέγιστο αριθμό αρχείων που το σύστημα θα συντηρεί (7).

2.4.2 Κονσόλα ISA Management

Από την κονσόλα ISA Management και από το μονοπάτι Servers and Arrays/Server/Monitoring/Alerts, παρακολουθούμε το χρόνο στον οποίο ο εξυπηρετητής έχει εκκινήσει τη λειτουργία του.

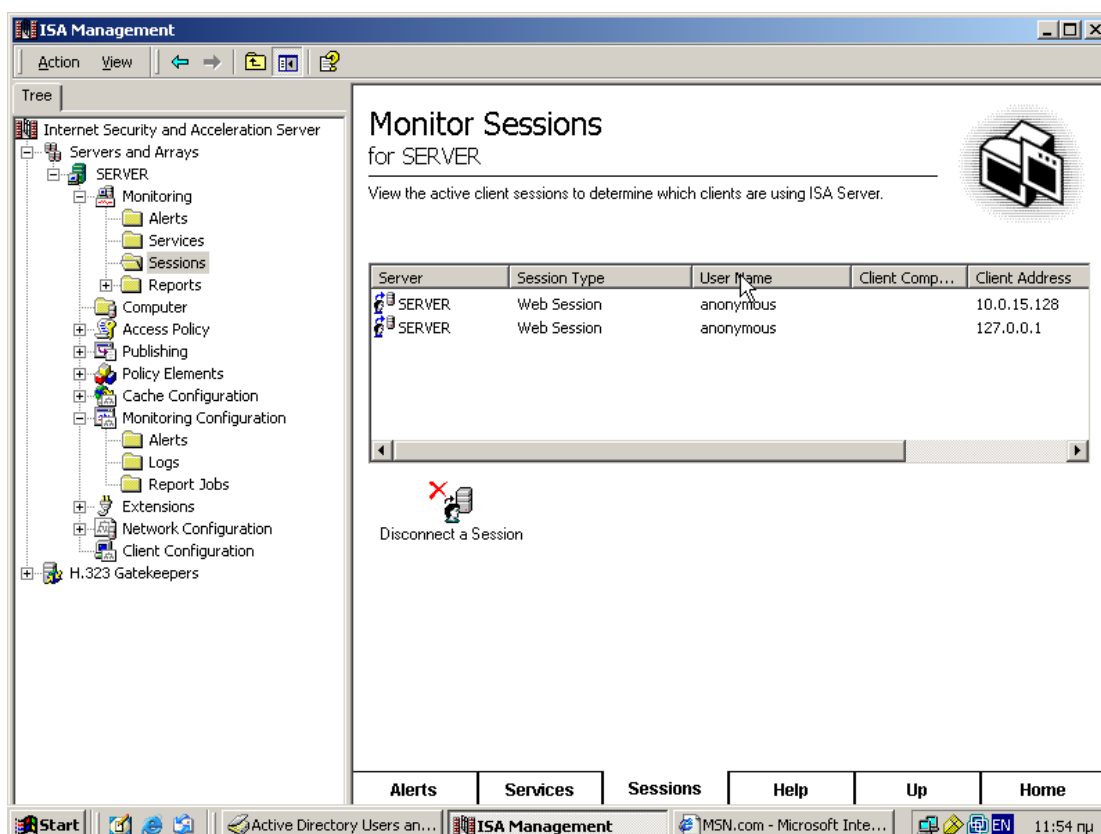


Από την κονσόλα ISA Management και από το μονοπάτι Servers and Arrays/Server/Monitoring/Services, παρακολουθούμε τα Services που έχει εκκινήσει ο ISA Server 2000 και την τρέχουσα κατάστασή τους. Στο παράδειγμα που ακολουθεί δύο σταθμοί επικοινωνούν μέσω web, κάτι που φαίνεται και στον αριθμό των Sessions (Number of Sessions). Επίσης στην κονσόλα φαίνεται και ο χρόνος όπου το service είναι λειτουργικό (Service Up Time).



Από την κονσόλα ISA Management και από το μονοπάτι Servers and Arrays/Server/Monitoring/Sessions, παρακολουθούμε αναλυτικά τα τρέχοντα / ενεργά Sessions, στα οποία φαίνεται:

- ο τύπος του session (Session Type)
- ο χρήστης που έχει ενεργοποιήσει το session. Στα σχολικά εργαστήρια η χρήση της υπηρεσίας proxy δεν απαιτεί authentication, οπότε οι χρήστες του domain παρόλο που έχουν κάνει login στο domain, φαίνονται στην ακόλουθη κονσόλα ως anonymous
- και η διεύθυνση του σταθμού του χρήστη απ' όπου κάνει την αίτηση σύνδεσης.



The screenshot shows the ISA Management console with the 'Monitor Sessions' page selected. The left-hand tree view shows the navigation path: Internet Security and Acceleration Server > Servers and Arrays > SERVER > Monitoring > Sessions. The main content area is titled 'Monitor Sessions for SERVER' and includes the instruction 'View the active client sessions to determine which clients are using ISA Server.' Below this is a table with the following data:

Server	Session Type	User Name	Client Comp...	Client Address
SERVER	Web Session	anonymous		10.0.15.128
SERVER	Web Session	anonymous		127.0.0.1

Below the table, there is a button labeled 'Disconnect a Session' with a red 'X' icon. At the bottom of the console, there are navigation buttons for Alerts, Services, Sessions, Help, Up, and Home. The taskbar at the bottom shows the Start button, several application icons, and the system tray with the time 11:54 μμ.

2.4.3 Αναφορές

Αναφορές λειτουργίας του ISA Server δημιουργούμε από την κονσόλα ISA Management και από το μονοπάτι: “SERVER/Monitoring Configuration/Report Jobs”. Με Δεξί κουμπί “New/Report Job ...” όπου ορίζουμε όνομα αναφοράς, την περίοδο δημιουργίας τους και στοιχεία χρονοπρογραμματισμού τους.

Τις αναφορές τις βλέπουμε από το μονοπάτι “SERVER/Monitoring/Reports”. Για κάθε αναφορά δημιουργούνται τα ακόλουθα διαφορετικά views Summary, Web Usage, Application Usage, Traffic & Utilization, Security.

Ως σημαντικότερα σημεία των παραγόμενων αναφορών για το σχολικό εργαστήριο παρουσιάζουμε τα ακόλουθα:

Web Usage: Top Web Sites. Ο υπεύθυνος του εργαστηρίου μπορεί να διαπιστώσει αν το εργαστήριο χρησιμοποιείται για προβολή ακατάλληλου περιεχομένου, ώστε να το δηλώσει στην υπηρεσία Cache του ΠΣΔ. Η αναφορά έχει τη μορφή του ακόλουθου παραδείγματος, στο οποίο για συντομία παρουσιάζονται μόνο οι πρώτες δέκα γραμμές.

No	Site	Unique Users	Requests	% of Total Requests	Bytes In	% of Total Bytes In	Bytes Out	% of Total Bytes Out	Total Bytes	% of Total Bytes
1	ftp.ntua.gr	1	3	0,3 %	354,9 MB	95,3 %	783,0 B	0,2 %	354,9 MB	95,2 %
2	www.sch.gr	1	172	18,9 %	452,5 KB	0,1 %	95,4 KB	21,0 %	548,0 KB	0,1 %
3	www.in.gr	1	149	16,4 %	459,1 KB	0,1 %	56,1 KB	12,3 %	515,1 KB	0,1 %
4	www.safer-networking.org	1	77	8,5 %	317,4 KB	0,1 %	25,5 KB	5,6 %	342,9 KB	0,1 %
5	stb.msn.com	2	58	6,4 %	279,2 KB	0,1 %	29,6 KB	6,5 %	308,8 KB	0,1 %
6	www.msn.com	2	5	0,5 %	186,1 KB	0,0 %	2,8 KB	0,6 %	189,0 KB	0,0 %
7	www.ntua.gr	1	32	3,5 %	143,6 KB	0,0 %	9,3 KB	2,0 %	152,8 KB	0,0 %
8	www.microsoft.com	1	24	2,6 %	143,9 KB	0,0 %	6,9 KB	1,5 %	150,7 KB	0,0 %
9	stc.msn.com	2	58	6,4 %	100,0 KB	0,0 %	31,1 KB	6,8 %	131,2 KB	0,0 %
10	stj.msn.com	2	12	1,3 %	111,4 KB	0,0 %	6,2 KB	1,4 %	117,7 KB	0,0 %
	All Others		160	17,6 %	244,1 KB	0,1 %	82,1 KB	18,1 %	326,1 KB	0,1 %
	Total	4	911	100,0 %	372,3 MB	100,0 %	454,3 KB	100,0 %	372,7 MB	100,0 %

Traffic and Utilization: Cache Performance. Παρουσιάζεται η απόδοση του μηχανισμού proxy (πόσα δεδομένα ήρθαν από την cache και πόσα από το internet), τα οποία υπολογίζονται τόσο σε αριθμό αιτήσεων όσο και σε μέγεθος δεδομένων.

Status	Requests	% of Requests	Total Bytes
Objects returned from the Internet	590	64,8 %	357,4 MB
Objects returned from cache without verification	110	12,1 %	14,6 MB
Objects returned from the Internet, updating a file in cache	44	4,8 %	296,5 KB
Information not available	29	3,2 %	29,3 KB
Objects returned from cache after verifying that they have not changed	138	15,1 %	26,5 KB
Total	911	100 %	372,3 MB

Traffic and Utilization: Processing Time. Παρουσιάζεται ο συνολικός χρόνος CPU ανά ώρα της ημέρας, στοιχείο που μπορεί να χρησιμοποιηθεί για να αξιολογηθεί η απόδοση και η επιβάρυνση του server για την υποστήριξη της λειτουργίας proxy.

Time	Interval	Average Processing Time
10/30/2007	00:00	-
10/30/2007	01:00	-
10/30/2007	02:00	-
10/30/2007	03:00	-
10/30/2007	04:00	-
10/30/2007	05:00	-
10/30/2007	06:00	-
10/30/2007	07:00	-
10/30/2007	08:00	-
10/30/2007	09:00	0,0 sec

10/30/2007	10:00	0,4 sec
10/30/2007	11:00	0,1 sec
10/30/2007	12:00	0,2 sec
10/30/2007	13:00	0,3 sec
10/30/2007	14:00	0,6 sec
10/30/2007	15:00	-
10/30/2007	16:00	-
10/30/2007	17:00	-
10/30/2007	18:00	-
10/30/2007	19:00	-
10/30/2007	20:00	-
10/30/2007	21:00	-
10/30/2007	22:00	-
10/30/2007	23:00	-

Traffic and Utilization: Errors. Στη συγκεκριμένη αναφορά καταγράφονται τα λάθη κατά την επικοινωνία του server με το Internet.

2.4.4 Παρακολούθηση απόδοσης

Μέσω του ISA Server Performance Monitor (από το Start menu), όπου είναι συγκεντρωμένες όλες οι παράμετροι του συστήματος που σχετίζονται με τη λειτουργία του ISA Server.

Κατά την περίοδο όπου ο ISA Server 2000 παρουσιάζει κάποιο πρόβλημα στην απόδοσή του, το Performance Monitor μπορεί να αξιοποιηθεί για να εντοπιστούν οι παράμετροι του συστήματος που δεν αποκρίνονται ικανοποιητικά.

2.5 Κοινά Προβλήματα

2.5.1 Οι σταθμοί εργασίας δε μπορούν να προσπελάσουν FTP sites μέσω του ISA Server 2000.

Αυτή η δυσλειτουργία μπορεί να παρουσιάζεται όταν σταθμοί εργασίας προσπαθούν μέσω του ISA Server 2000 να προσπελάσουν ένα FTP site, έχοντας ενεργοποιημένη στον Internet Explorer τη ρύθμιση “Enable folder view for FTP sites”.

Όταν ο Internet Explorer έχει ενεργοποιημένη αυτή τη ρύθμιση παρακάμπτει τον ISA Server και προσπαθεί να στείλει το αίτημα σύνδεσης του πρωτοκόλλου FTP απευθείας στο Internet. Λόγω της εγκατάστασης και λειτουργίας του ISA Server αυτή η απόπειρα αποτυγχάνει.

Για να αντιμετωπιστεί το πρόβλημα απενεργοποιούμε την ανωτέρω ρύθμιση μέσω της επιλογής του Internet Explorer “Tools/Internet Options/Advanced Tab/clear Enable folder view for FTP sites/Apply/OK”.

3 Βιβλιογραφία

1. [How to obtain the latest Internet Security and Acceleration Server 2000 service pack](#)
2. [Automatic Discovery for Firewall and Web Proxy Clients](#)
3. [How to connect your company to the Internet by using ISA Server 2000 with Windows 2000](#)
4. [Internal clients cannot use Internet Explorer to access FTP sites through Microsoft Proxy Server or Internet Security and Acceleration Server 2000](#)
5. [How To Configure Logging in Internet Security and Acceleration Server](#)
6. [The Report Logs Record Anonymous Logon Attempts When Logging Is Enabled for the Web Proxy Service \(όχι\)](#)
7. [How to Delete the Web Cache on Internet Security and Acceleration Server](#)