ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

CITRIX NETSCALER – Security for next generation data centers based on cloud

Ασφάλεια υπολογιστικών υποδομών που υλοποιούνται σε νεφοϋπολογιστικά περιβάλλοντα

Επιβλέπων Καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

Ονοματεπώνυμο Φοιτητή: Χρήστος Κουτσογιάννης

ΑΜ: 1212

Ημερομηνία παράδοσης: Ιούνιος 2016

Πειραιάς 2016

Περίληψη

Η παρούσα διπλωματική εργασία δημιουργήθηκε για να παρουσιάσει την ασφάλεια που παρέχεται σε υπολογιστικές υποδομές που υλοποιούνται σε νεφοϋπολογιστικά περιβάλλοντα αλλά και να αναδείξει τρόπους βελτίωσης αυτής. Πιο συγκεκριμένα βασίζεται στην υλοποίηση υποδομής Citrix XenApp και XenDesktop σε περιβάλλον Microsoft Azure, στην λειτουργία αυτής και στις μεθόδους ασφαλείας που διαθέτει. Τέλος αναδεικνύεται η συμπεριφορά της υποδομής σε διάφορες εκτελέσεις επιθέσεων που λαμβάνουν μέρος μέσω υπολογιστικών συστημάτων Linux.

Abstract

The current Thesis has been created to present the security standards given by next generation data centers based on cloud, as well as to point out the way to improve them. Specifically it is based on the implementation and operation of Citrix environment, relying on Microsoft Azure Cloud, furthermore on the security methods that are provided. At last highlights the behavior of the infrastructure in various attacks which are executed via Linux based systems.

Περιεχόμενα

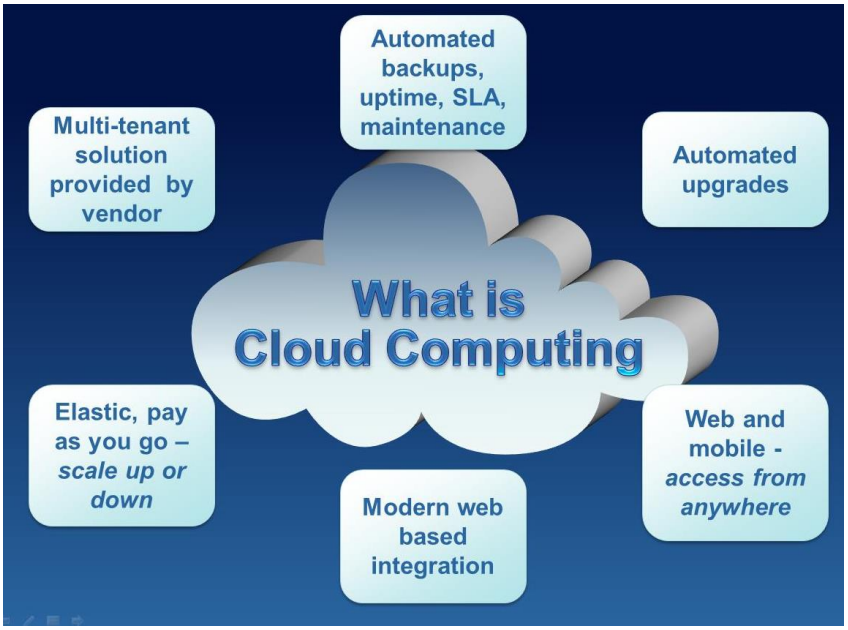
Πίνακας Εικόνων

Λίστα Πινάκων

1 Εισαγωγή

Στην σημερινή εποχή όπου η τεχνολογική ανάπτυξη είναι ραγδαία, ένας πολύ σημαντικός τομέας ο οποίος γιγαντώνεται συνεχώς είναι το cloud computing και οι υπηρεσίες που δίδονται μέσω αυτής της τεχνολογίας.

Στην προκειμένη περίπτωση, μιλώντας για cloud αναφερόμαστε στην τεχνολογία που επιτρέπει στον χρήστη να χρησιμοποιεί υπηρεσίες όπως λογισμικό, αποθηκευτικό χώρο ή ακόμα και υπολογιστικούς πόρους ανάλογα με τις ανάγκες του, συνδεόμενος μέσω του διαδικτύου στον πάροχο ο οποίος παρέχει τις υπηρεσίες αυτές, οι σπουδαιότεροι - κολοσσοί πάροχοι τέτοιων υπηρεσιών είναι οι: Google, Microsoft-Azure, Amazon, IBM.



Εικόνα 1-1. Cloud Computing

1.1 Είδη υπηρεσιών Cloud Computing

Τα είδη των υπηρεσιών cloud computing χωρίζονται στις παρακάτω κατηγορίες η καθεμία από τις οποίες εξυπηρετεί διαφορετικές ανάγκες και προσφέρουν υπηρεσίες προσαρμοσμένες στις απαιτήσεις του πελάτη.

Software-as-a-Service (SaaS), αφορά την υπενοικίαση λογισμικού χωρίς να υπάρχει ανάγκη αγοράς άδειας χρήσης από τον πελάτη, αλλά πληρωμής ανάλογα με την χρήση που κάνει. Πιο συγκεκριμένα, μία εφαρμογή βρίσκεται εγκατεστημένη σε έναν server και είναι προσβάσιμη από τον χρήστη μέσω του διαδικτύου χρησιμοποιώντας κάποιον browser over **S**ecure **S**ockets **L**ayer για την ασφάλεια των εφαρμογών. Τα

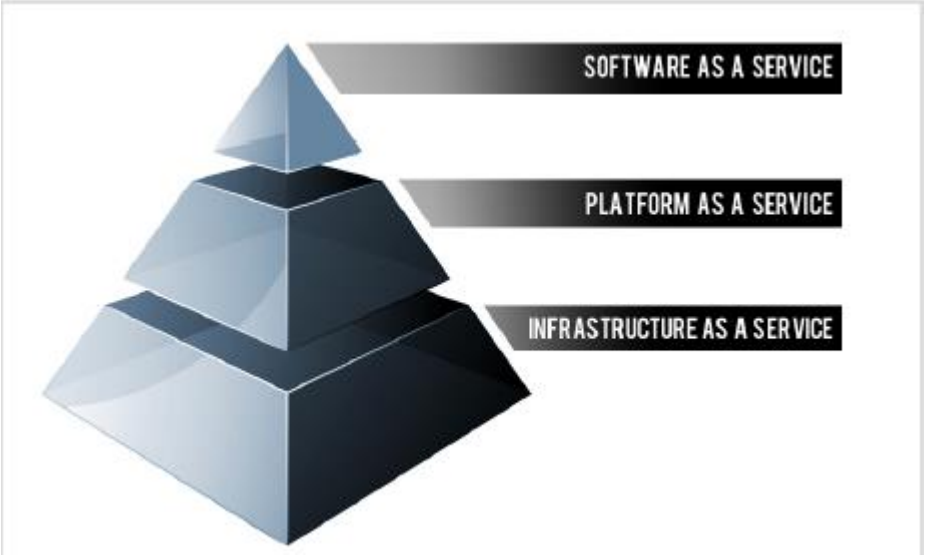
κυριότερα πλεονεκτήματα του συγκεκριμένου είδους είναι, η μεγάλη ευελιξία, η ποιότητα των υπηρεσιών, η υψηλή σταθερότητα αλλά και οι ελάχιστες απαιτήσεις συντήρησης. Τέτοιου είδους υπηρεσίες είναι: Microsoft Exchange online, Microsoft SharePoint online, Google Apps, Citrix GoToMeeting, Citrix XenApp.

Desktop-as-a-Service (DaaS), ο πάροχος της υπηρεσίας προσφέρει εικονική υποδομή στον πελάτη “Virtual Desktop Infrastructure (VDI)” δίνοντας έτσι την δυνατότητα στον πελάτη-οργανισμό να απαλλαγεί από το κόστος αναβάθμισης των μηχανημάτων-desktops που υπάρχουν εντός του οργανισμού. Ο χρήστης με αυτόν τον τρόπο έχει τη δυνατότητα χρήσης του VDI από οποιαδήποτε συσκευή διαθέτει και από οποιαδήποτε τοποθεσία βρίσκεται μέσω του διαδικτύου. Ο πάροχος είναι υπεύθυνος για την διαχείριση της υποδομής ενώ ανάλογα με τις ανάγκες του πελάτη δίδεται και το επιθυμητό από αυτόν επίπεδο διαχείρισης των υπηρεσιών της υποδομής. Με την υπηρεσία αυτή προσφέρεται αυξημένη ασφάλεια δεδομένων, ευελιξία σε τυχόν ανάγκες του πελάτη για αναβάθμιση των υπηρεσιών αλλά και βελτιωμένη ανάκτηση από πιθανή καταστροφή. Οι σημαντικότεροι πάροχοι της συγκεκριμένης υπηρεσίας είναι: VMware Horizon Air, Amazon WorkSpaces, Citrix XenDesktop.

Platform-as-a-Service, όπου παρέχεται μια πλατφόρμα εφαρμογών για πελάτες οι οποίοι εξειδικεύονται στην ανάπτυξη λογισμικού, έτσι δίνεται η ευκαιρία στον ενδιαφερόμενο να αναπτύξει, δοκιμάσει, να διαθέσει και να συντηρήσει εφαρμογές σε ένα ενιαίο περιβάλλον. Το λειτουργικό και η πλατφόρμα παρέχεται στον πελάτη χωρίς να χρειάζεται αυτός να ασχοληθεί με την συντήρηση αυτού έχοντας όμως περιορισμένη πρόσβαση στο λειτουργικό κάτι που σημαίνει ότι δεν μπορεί να το ελέγξει λεπτομερώς. Το κόστος αυτής της υπηρεσίας βασίζεται στο μοντέλο pay-per-use μέσω του οποίου επιτυγχάνεται η πλήρης αξιοποίηση των υπολογιστικών πόρων που πραγματικά χρειάζεται ο πελάτης σε σχέση με το κόστος. Με αυτόν τον τρόπο επιτυγχάνεται η διάθεση υπηρεσιών σε οποιαδήποτε μεταβολή των αναγκών του πελάτη ως προς την διάθεση πόρων όπως μνήμη, ισχύς, αποθηκευτικός χώρος, bandwidth, κάτι που καθιστά την συγκεκριμένη υπηρεσία πλήρως ευέλικτη. Παραδείγματα τέτοιου είδους υπηρεσιών είναι: Microsoft SQL Azure, Windows Azure AppFabric, Apprenda, Google App Engine.

Infrastructure-as-a-Service, δίνεται η δυνατότητα στον πελάτη να δεσμεύσει επεξεργαστική ισχύ, δίκτυα, αποθηκευτικά μέσα και άλλους υπολογιστικούς πόρους από τον πάροχο. Σε αυτήν την περίπτωση ο πελάτης έχει την δυνατότητα πλήρους ελέγχου των λειτουργικών συστημάτων των αποθηκευτικών μέσων και των εφαρμογών που έχουν αναπτυχθεί και είναι υπεύθυνος για την διαχείριση αυτών.

Όπως και στην περίπτωση του PaaS το κόστος βασίζεται στις απαιτήσεις του πελάτη την συγκεκριμένη στιγμή με δυνατότητα πλήρους ευελιξίας “pay as you go”. Κάποια παραδείγματα τέτοιων υπηρεσιών είναι: Amazon EC2, Windows Azure, Rackspace, Google Compute Engine.



Εικόνα 1-2. Cloud Computing Stack

1.2 Μοντέλα ανάπτυξης Cloud Computing

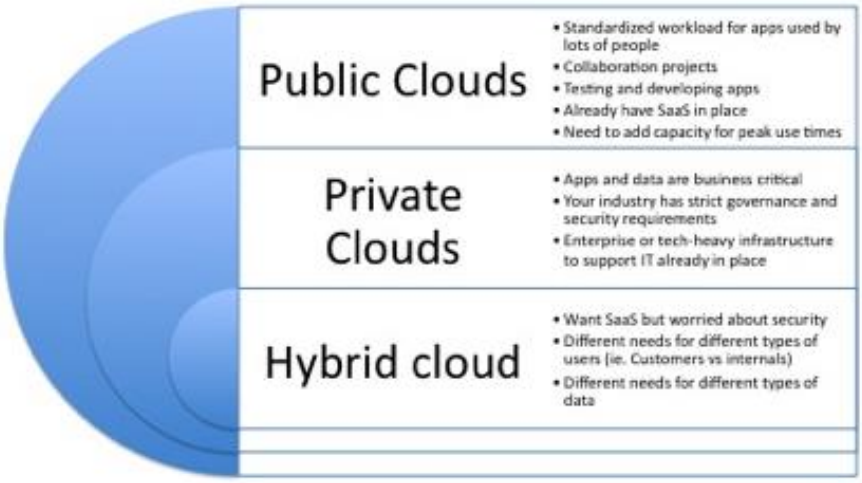
Το cloud computing μπορεί να ταξινομηθεί σε τρία βασικά μοντέλα και αυτό γίνεται με βάση την αρχιτεκτονική, την τοποθεσία όπου βρίσκεται το data center, το είδος των δεδομένων που ανταλλάσσονται, αλλά και το επίπεδο ασφάλειας και διαχείρισης που επιθυμεί ο πελάτης.

Public cloud, στο συγκεκριμένο μοντέλο η υποδομή φιλοξενείται σε data centers του παρόχου, ο πελάτης δεν έχει καμία δικαιοδοσία στον χώρο όπου αυτή φιλοξενείται καθώς η συντήρηση και η υποστήριξη είναι ευθύνη του παρόχου, ενώ η υποδομή είναι κοινή και διαμοιράζεται μεταξύ πολλών οργανισμών-πελατών βεβαίως με τους κατάλληλους περιορισμούς έτσι ώστε να καθιστά ασφαλή την χρήση της. Οι πόροι που κατανέμονται από τον πάροχο αναλογούν στις ανάγκες του πελάτη με την δυνατότητα αύξησης ή μείωσης αυτών να είναι ένα βασικό πλεονέκτημα (pay-per-use model). Αυτό το μοντέλο ενδείκνυται για εφαρμογές τις οποίες χρησιμοποιεί μεγάλος αριθμός χρηστών όπως e-mail, όπως επίσης και για εφαρμογές όπου είναι απαραίτητη η αύξηση υπολογιστικών πόρων σε ώρες αιχμής.

Private Cloud, σε αυτό το μοντέλο η υποδομή είναι ειδικά προσαρμοσμένη για τον πελάτη και διαχειρίσιμη εντός ενός ιδιωτικού δικτύου όπου ο πελάτης είναι υπεύθυνος για την διαχείριση της υποδομής και των εφαρμογών. Συγκριτικά με το public μοντέλο υπερισχύει σε σχέση με την ασφάλεια αλλά υστερεί λόγω

μεγαλύτερου κόστους. Η χρήση του μοντέλου προτείνεται για μεγάλους οργανισμούς-πελάτες που έχουν την δυνατότητα να διαχειριστούν αποτελεσματικά μία τέτοια υποδομή, με κύριο μέλημα την ασφάλεια των δεδομένων και των εφαρμογών που οι χρήστες διαχειρίζονται.

Hybrid Cloud, είναι ο συνδυασμός private και public cloud, έτσι επιτυγχάνεται η πλήρης εκμετάλλευση όλων των πλεονεκτημάτων των δύο μοντέλων. Έτσι ο πελάτης μπορεί να κάνει χρήση μιας εφαρμογής για την οποία υπάρχουν λιγότερα ζητήματα ασφαλείας μέσω public cloud ενώ ταυτόχρονα μιας πιο κρίσιμης εφαρμογής ευαίσθητης σε θέματα ασφάλειας μέσω του private cloud. Επίσης μία πιο πολύπλοκη λύση μέσω hybrid cloud είναι η χρήση μιας εφαρμογής μέσω public και η αποθήκευση των ευαίσθητων δεδομένων στο private cloud, έτσι θα επιτευχθεί η ασφάλεια των δεδομένων (private) αλλά και η δυνατότητα ευελιξίας στη κατανομή υπολογιστικών πόρων όταν η απαιτήσεις για την ομαλή λειτουργία της εφαρμογής αυξάνονται κατά τις ώρες αιχμής (public).



Εικόνα 1-3. Cloud Basic Models

1.3 Οφέλη σε επίπεδο ασφάλειας

Η τεχνολογία cloud computing οδηγεί στην εξέλιξη της πληροφορικής όπως την ξέραμε έως πρότινος και αυτό συνεπάγεται και στην εξέλιξη της ασφάλειας των υπολογιστικών συστημάτων με πολλά οφέλη ως προς αυτήν.

Τα μέτρα ασφαλείας όπως filtering, patch management, hardening of hypervisors κλπ, είναι πιο φθηνά όταν παρέχονται σε μεγάλης κλίμακας υποδομές.

Η ασφάλεια αποτελεί προτεραιότητα για πολλούς πελάτες οι οποίοι θα επιλέξουν και θα αγοράσουν λύσεις από τον πάροχο για την εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της ανθεκτικότητας των δεδομένων, αυτό σημαίνει συγκέντρωση

υψηλής ποιότητας τεχνογνωσίας για τον πάροχο και βελτίωση των τεχνικών ασφαλείας.

Οι ενημερώσεις και αναβαθμίσεις σχετικά με κακόβουλο λογισμικό και κακόβουλων ενεργειών μπορούν να γίνουν πιο αποτελεσματικά και έγκαιρα σε μία ενιαία ομογενή πλατφόρμα σε σχέση με τα παραδοσιακά client-based συστήματα.

Η ικανότητα του παρόχου να κατανέμει δυναμικά υπολογιστικούς πόρους για υπηρεσίες όπως filtering, authentication, encryption είναι ένα σημαντικό πλεονέκτημα.

Τέλος η συγκέντρωση των υπολογιστικών πόρων σε ένα σημείο, που προκύπτει από το cloud computing οδηγεί στη χρήση λιγότερων διεργασιών ασφαλείας και ελέγχων φυσικής πρόσβασης με αποτέλεσμα την μείωση του κόστους.

1.4 Στόχος και δομή της εργασίας

Η παρούσα διπλωματική εργασία έχει ως στόχο την ανάλυση της τεχνολογίας cloud computing χρησιμοποιώντας την υπηρεσία Infrastructure-as-a-Service που παρέχεται από την Microsoft – Azure αλλά και της υπηρεσίας Software-as-a-Service και *Desktop-as-a-Service* μέσω Citrix XenApp και XenDesktop αντίστοιχα.
Ως κύριος στόχος ορίζεται η παραμετροποίηση του Citrix Netscaler που είναι ο συνδετικός κρίκος μεταξύ του χρήστη και της υποδομής και είναι το λειτουργικό που είναι εκτεθειμένο στο internet και σε κάθε είδους κυβερνο-επιθέσεις, έτσι ώστε να καταστεί όσο το δυνατόν ασφαλέστερη η υπηρεσία που δίδεται από την υποδομή.

Η εργασία είναι οργανωμένη σε πέντε κεφάλαια,

Στο *1ο Κεφάλαιο* δίδεται μία εισαγωγική αναφορά στο cloud computing
Στο *2ο Κεφάλαιο* αναλύονται οι υπηρεσίες Citrix XenApp και XenDesktop και η ασφάλεια που αυτές παρέχουν
Στο *3ο Κεφάλαιο* γίνεται ανάλυση του Citrix Netscaler
Στο *4ο Κεφάλαιο* δίδονται λεπτομέρειες σχετικά με την σχεδίαση της υποδομής και της παραμετροποίησης του Netscaler
Ενώ στο *5ο Κεφάλαιο* καταγράφονται τα συμπεράσματα που διεξήχθησαν από τις παραπάνω ενέργειες

2 Citrix Cloud – XenApp and XenDesktop

Η εταιρεία Citrix είναι ένας παγκόσμιος κολοσσός που διαθέτει μία από τις πιο σύγχρονες πλατφόρμες cloud computing με σκοπό την διάθεση υπηρεσιών cloud όπως applications (software as a service), desktops (desktop as a service), mobile και web services στον τελικό χρήστη, μέσω οποιουδήποτε τύπου cloud (public, private ή hybrid).

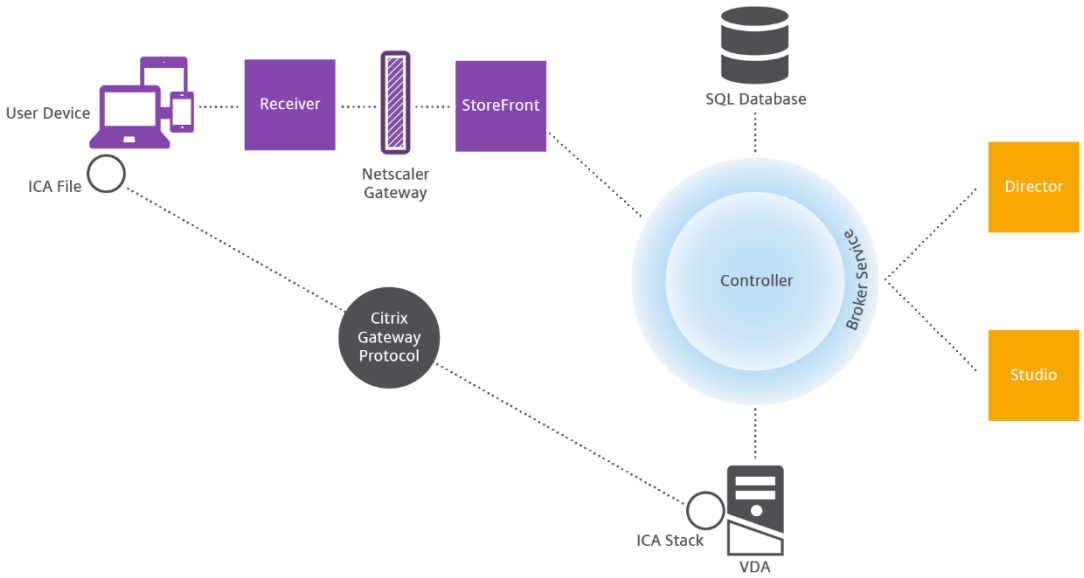
Αναπτυσσόμενη σε data centers ή στο cloud η πλατφόρμα Citrix προσφέρει:
Ασφάλεια, έναντι επιθέσεων DDos, SQL injection, XSS, SSL, διασφαλίζοντας το PCI DSS standard. Καθώς προσφέρει κεντρικοποιημένη παροχή εφαρμογών, διασφαλίζοντας τα δεδομένα στο datacenter, ενώ δίνει την δυνατότητα στους διαχειριστές να προσαρμόζουν την πρόσβαση που έχει ο κάθε χρήστης σε κάθε εφαρμογή εξασφαλίζοντας την ασφάλεια πολύτιμων πληροφοριών.
Αξιοπιστία, διανέμοντας κάθε εφαρμογή με ασφάλεια και παρέχοντας αναλυτικά δικτυακά στοιχεία για κάθε κίνηση σε επίπεδο mobile, web και desktop.
Βελτιωμένες επιδόσεις, σε εφαρμογές που χρησιμοποιούνται από mobile,remote ή branch χρήστες. Παρέχοντας εξαιρετικές αποδόσεις σε γραφικά και πολυμέσα ανεξάρτητα των δυνατοτήτων της τελικής συσκευής, αυξάνοντας έτσι την παραγωγικότητα του τελικού χρήστη.
Ευελιξία, διασφαλίζοντας την επιχειρηματική συνέχεια και την αποκατάσταση καταστροφής υποδομών πληροφοριακών συστημάτων (disaster recovery plan), όπως επίσης και την αύξηση των υπολογιστικών πόρων όταν αυτό κρίνεται αναγκαίο για την καλύτερη υποστήριξη του πελάτη.
Εξοικονόμηση κόστους, εδραιώνοντας λύσεις απομακρυσμένης πρόσβασης και εξαλείφοντας το κόστος των WAN δικτύων.
Επίσης η διαχείριση ενός κεντρικοποιημένου συστήματος, όπως αυτό που δίνει η τεχνολογία Citrix, υπερτερεί σε σχέση με ξεχωριστά διανεμημένα συστήματα πληροφορικής τόσο σε εξοικονόμηση κόστους, όσο και σε ασφάλεια, ευελιξία αλλά και αξιοπιστία.

2.1 Επισκόπηση XenApp και XenDesktop

Οι τεχνολογίες XenApp και XenDesktop δίνουν την δυνατότητα:

- ο τελικός χρήστης να χρησιμοποιεί εφαρμογές και desktops ανεξάρτητα από τα χαρακτηριστικά της συσκευής που χρησιμοποιεί
- ο administrator να παρέχει περιορισμένη πρόσβαση σε χρήστες ή συσκευές αλλά και να διαχειρίζεται όλο το δίκτυο από ένα μοναδικό data center.

Η αρχιτεκτονική που χρησιμοποιείται για την υλοποίηση των τεχνολογιών αυτών ονομάζεται FlexCast Management Architecture (FMA), βασικό χαρακτηριστικό της οποίας είναι η δυνατότητα να εκτελούνται διαφορετικές εκδόσεις XenApp και XenDesktop από ένα “single site”. Τα βασικά στοιχεία της αρχιτεκτονικής αυτής είναι τα παρακάτω.



Εικόνα 2-1. Deployment Overview

2.1.1 Τα κύρια μέρη της αρχιτεκτονικής FMA

Citrix Receiver
Είναι μία εφαρμογή τύπου “software-client” που εγκαθίσταται στην συσκευή του χρήστη μέσω της οποίας γίνεται η σύνδεση με το εικονικό μηχάνημα (virtual machine) κάνοντας χρήση των πορτών TCP 80 ή 443 και επικοινωνεί με το Storefront χρησιμοποιώντας το StoreFront Service API.

Citrix StoreFront
Το interface μέσω του οποίου γίνεται ο έλεγχος ταυτότητας του χρήστη, η διαχείριση των εφαρμογών και των desktops. Επίσης εκεί φιλοξενείται και το application store. Το Storefront επικοινωνεί με το Delivery Controller χρησιμοποιώντας αρχεία XML.

Delivery Controller
Το κεντρικό εργαλείο διαχείρισης ενός XenApp ή XenDesktop site, αποτελούμενο από services διαχείρισης πόρων, εφαρμογών και desktops. Πολύ σημαντική λειτουργία είναι η εξισορρόπηση των φορτίων που προκαλούνται από τις συνδέσεις των χρηστών “load balancing”

Virtual Delivery Agent (VDA)

Είναι ο agent ο οποίος είναι εγκατεστημένος σε μηχανήματα με λειτουργικό σύστημα Windows server και καθιστά τα μηχανήματα αυτά και τους πόρους που φιλοξενούνται σε αυτά, διαθέσιμα στους χρήστες. Έτσι ο agent επιτρέπει σε αυτά τα συστήματα να φιλοξενούν πολλαπλές συνδέσεις χρηστών μέσω των παρακάτω πορτών:

- TCP port 80 ή 443, το οποίο προϋποθέτει ενεργοποίηση του πρωτοκόλλου “Transport Layer Security”
- TCP port 2598, που προϋποθέτει ενεργοποίηση του πρωτοκόλλου “Citrix Gateway Protocol” που είναι υπεύθυνο για την αξιοπιστία της διασύνδεσης του χρήστη “user session[1]”
- TCP port 1494 σε περίπτωση που το πρωτόκολλο CGP είναι απενεργοποιημένο

Broker Service
Είναι το service που ελέγχει ποιος χρήστης είναι συνδεδεμένος και σε ποιον server, ποιους πόρους χρησιμοποιεί και αν ο χρήστης πρέπει να επανασυνδεθεί σε μια εφαρμογή στην οποία ήταν ήδη συνδεδεμένος και αποσυνδέθηκε πριν από κάποιο διάστημα. Το Broker Service εκτελεί εντολές powershell και επικοινωνεί με τον Broker Agent στην πόρτα TCP 80.

Broker agent
Φιλοξενεί πολλαπλά plugins και συλλέγει δεδομένα σε πραγματικό χρόνο, βρίσκεται στο VDA και συνδέεται μέσω της πόρτας 80 στον Delivery Controller.

Monitor Service
Είναι ένα στοιχείο του Delivery Controller υπεύθυνο για την συλλογή δεδομένων ιστορικού τα οποία και αποθηκεύονται στην SQL βάση δεδομένων, χρησιμοποιώντας την πόρτα 80 ή 443.

ICA File/Stack
Είναι απαραίτητο για την ομαδοποίηση των πληροφοριών του χρήστη που είναι απαραίτητες για την σύνδεση με το VDA.

Site Database
Η βάση δεδομένων “Microsoft SQL Server database” στην οποία αποθηκεύονται δεδομένα που χρησιμοποιούνται από τον Delivery Controller, όπως Site policies, Machine Catalogs, and Delivery Groups.

Netscaler Gateway
Μία λύση η οποία παρέχει ασφαλής σύνδεση με επιπρόσθετες πιστοποιήσεις ασφαλείας. Αναλυτικότατη περιγραφή δίδεται στο κεφάλαιο 3.

Citrix Director

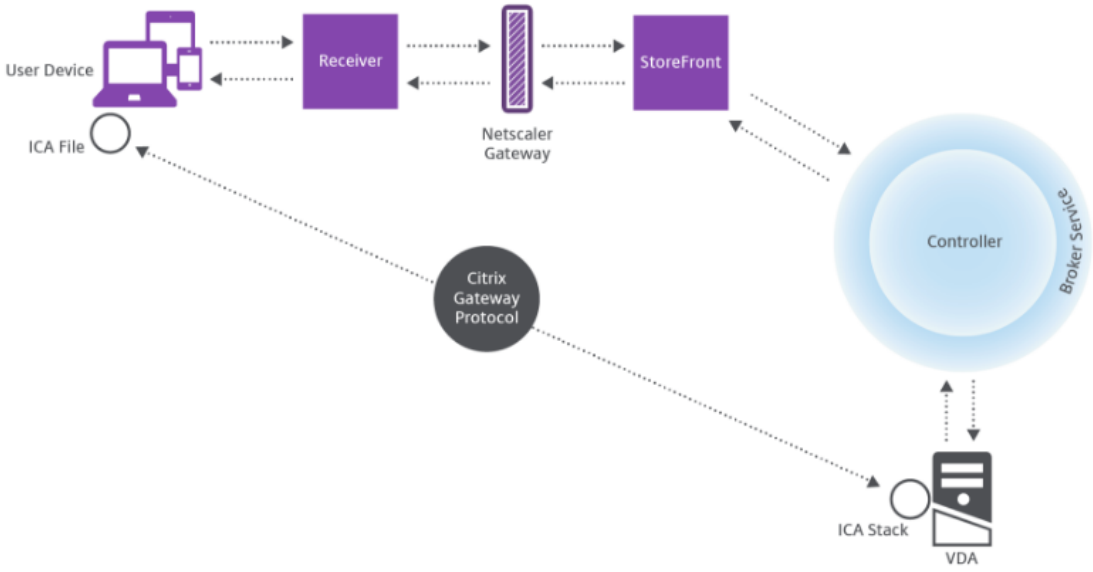
[1] η ανταλλαγή διαδραστικής πληροφορίας μεταξύ ενός χρήστη και μίας συσκευής σε ένα ορισμένο χρονικό διάστημα

Ένα “web-based” εργαλείο που επιτρέπει στους administrators την πρόσβαση σε δεδομένα πραγματικού χρόνου. Τα δεδομένα αυτά προέρχονται από τον Broker Agent, από την βάση δεδομένων καθώς και από τον Netscaler. Χρησιμοποιούνται κατά βάση για την υποστήριξη των χρηστών και την επίλυση πιθανών προβλημάτων που έχουν προκύψει ενώ επικοινωνεί επίσης με τον Controller στην πόρτα 80 ή 443.

Citrix Studio
Μία κονσόλα διαχείρισης που δίνει τη δυνατότητα στον administrator να ρυθμίσει και να διαχειριστεί sites και του δίνει πρόσβαση σε δεδομένα πραγματικού χρόνου μέσω του Broker Agent. Η επικοινωνία με τον Controller γίνεται μέσω της πόρτας 80.

2.1.2 Πως διαχειρίζονται οι συνδέσεις των χρηστών

Η σύνδεση του χρήστη στο περιβάλλον Citrix XenApp ή XenDesktop, γίνεται είτε μέσω Citrix receiver ή Receiver for Web, που βρίσκονται εγκατεστημένα στην συσκευή του χρήστη. Αφού συνδεθεί επιτυχώς επιλέγει την virtual εφαρμογή ή desktop που χρειάζεται.



Εικόνα 2-2. Σύνδεση χρηστών

Τα στοιχεία του χρήστη δηλώνονται στον receiver και αφού γίνει η ταυτοποίηση αποκτά πρόσβαση στον Delivery Controller ο οποίος και καθορίζει ποιοι πόροι μπορούν να χρησιμοποιηθούν από τον χρήστη επικοινωνώντας με το Broker Service.

Η χρήση κάποιου SSL certification στο Storefront είναι πολύ σημαντική για την κρυπτογράφηση των στοιχείων του χρήστη που προέρχονται από τον Receiver.

Μετά την ολοκλήρωση της ταυτοποίησης του χρήστη η πληροφορία σχετικά με τις διαθέσιμες εφαρμογές ή desktops έρχεται από τον Controller στο Storefront και εμφανίζονται στο χρήστη μέσω του Receiver. Ο χρήστης επιλέγει κάποιο από τα

διαθέσιμα στοιχεία για αυτόν και ακολουθείται η αντίστροφη διαδρομή προς τον Controller ο οποίος καθορίζει τον κατάλληλο VDA όπου φιλοξενείται η εφαρμογή ή το desktop που επέλεξε ο χρήστης.

Ο Controller στέλνει ένα μήνυμα στον VDA που περιέχει τα στοιχεία του χρήστη και την πληροφορία σχετικά με την σύνδεση που επιθυμεί ο χρήστης, ο VDA δέχεται την πληροφορία και την επιστρέφει μέσω της ίδιας διαδρομής στον Receiver ο οποίος δημιουργεί ένα αρχείο ICA (Independent Computing Architecture) που αποθηκεύεται στη συσκευή του χρήστη, ενώ τα στοιχεία του χρήστη παραμένουν κρυπτογραφημένα από την στιγμή που έχει χρησιμοποιηθεί SSL Certification όπως είπαμε παραπάνω. Το αρχείο ICA δημιουργεί μία απευθείας σύνδεση μεταξύ της συσκευής του χρήστη και του VDA παρακάμπτοντας έτσι την διαδρομή Receiver-Storefront-Controller.

Στη σύνδεση μεταξύ Receiver-VDA χρησιμοποιείται το πρωτόκολλο Citrix Gateway Protocol, δίνοντας τη δυνατότητα μέσω ενός χαρακτηριστικού αξιοπιστίας (Session Reliability feature) σε περίπτωση που χαθεί η σύνδεση του χρήστη να γίνει η επανασύνδεση με τον VDA χωρίς να χρειαστεί να εφαρμοστεί από την αρχή η διαδικασία που περιεγράφηκε προηγουμένως.

Από την στιγμή που ο χρήστης συνδεθεί στον VDA τότε αυτός ενημερώνει τον Controller για την νέα σύνδεση, ο οποίος με την σειρά του στέλνει την πληροφορία στη βάση δεδομένων (Site Database) όπου καταγράφονται τα δεδομένα έτσι ώστε να είναι διαθέσιμη η πληροφορία για το Monitor service.

2.2 XenApp vs XenDesktop – Ποιο να επιλέξω?

Η κάθε εταιρεία έχει τις δικές της διαφορετικές ανάγκες όσον αφορά τις υπηρεσίες πληροφορικής που πρέπει να επιλέξει. Οι λύσεις XenApp και XenDesktop μπορούν να χρησιμοποιηθούν ξεχωριστά είτε συνδυαζόμενες για την καλύτερη εξυπηρέτηση των χρηστών. Πιο συγκεκριμένα, XenApp είναι μία λύση virtualization που βελτιστοποιεί την παραγωγικότητα δίνοντας τις απαραίτητες προσβάσεις σε εικονικές εφαρμογές, δεδομένα, desktops από οποιαδήποτε συσκευή, ενώ η τεχνολογία XenDesktop περιλαμβάνει τα ίδια χαρακτηριστικά συνδυάζοντας επιπλέον την λύση VDI όπως αναφέρθηκε παραπάνω.

Ο παρακάτω συγκριτικός πίνακας απεικονίζει τις υπηρεσίες που διαθέτουν τα προϊόντα XenApp-XenDesktop σε όλες τις εκδόσεις που είναι διαθέσιμες.

	XenApp Secure Browser	XenApp Advanced	XenApp Enterprise	XenApp Platinum	XenDesktop VDI	XenDesktop Enterprise	XenDesktop Platinum
XenApp published apps (Server-based hosted apps) can be deployed on 5 generations of Windows operating systems, enabling secure access to Windows apps on any type of device including iOS, Android, Mac and Windows devices for on-demand access from anywhere, lets users focus on work.		✔	✔	✔		✔	✔
XenApp published web and SaaS apps enables IT to select the best web browser for each web or SaaS app and securely deliver that app within that ideal browser to all users on any device, running any web browser.	✔	✔	✔	✔		✔	✔
XenApp published desktops are low-cost, locked-down virtual desktops that provide the flexibility and mobility benefits of desktop virtualization while maximizing IT control through enhanced security and simplified management.		✔	✔	✔		✔	✔
VDI desktops offer maximum user personalization of a persistent Windows virtual desktop that can be fully customized to meet the needs of your most-demanding users.					✔	✔	✔
VDI with Personal vDisk pairs the maximum user personalization benefits of VDI with the storage optimizations and administrative efficiencies of single image management to deliver a desktop virtualization solution that meets the needs of both users and IT admins.					✔	✔	✔
Server VDI enables enterprises and service providers the ability to deliver to an individual user a single session, server-based virtual desktop from the cloud.						✔	✔
Hosted physical desktops enable high performance remote access to physical desktops securely protected in the datacenter for optimal data protection, especially beneficial for graphically intensive applications that run best on a native OS that has direct access to the physical desktop hardware.						✔	✔
Remote PC Access (with Wake On LAN) instantly delivers desktop virtualization benefits without the need to migrate desktops to the datacenter by providing users with a secure, high-definition, direct connections to their office PCs.						✔	✔
Linux Hosted Shared Virtual Desktops XenApp and XenDesktop architecture supports Hosted Shared RHEL, SUSE and CentOS Linux Virtual Desktops.			✔	✔		✔	✔
Linux Dedicated VDI Desktops XenDesktop architecture supports RHEL, SUSE and CentOS Linux Dedicated VDI Desktops.						✔	✔
DesktopPlayer (Add-on*) extends the benefits of XenDesktop to Windows laptop and MacBook users, enabling them to run virtual desktops on a laptop whether they are online or offline. Employees gain freedom while IT gains control by centrally managing Windows virtual desktops deployed to corporate and BYO laptops. *Add-on purchase required						✔	✔
VM hosted apps ease Windows OS transitions and overcome application compatibility challenges by delivering virtual apps from a desktop operating system.			✔	✔		✔	✔

Πίνακας 2-1. Σύγκριση προϊόντων XenApp-XenDesktop

2.3 Ασφάλεια και Κανονιστική συμμόρφωση

Η τεχνολογία Citrix είναι έτσι σχεδιασμένη ώστε να προστατεύει τις πιο ευαίσθητες πληροφορίες, δίνοντας παράλληλα την επιλογή διαχείρισης των εφαρμογών και πρόσβασης στα δεδομένα από οποιαδήποτε τοποθεσία, δίκτυο και συσκευή. Έτσι όλοι οι εμπλεκόμενοι έχουν την δυνατότητα ασφαλής πρόσβασης είτε μέσω απομακρυσμένης πρόσβασης, κινητών συσκευών ή από το γραφείο. Στους οργανισμούς που διαθέτουν λύσεις Citrix παρέχεται το απαραίτητο επίπεδο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων χωρίς περιορισμούς στον τρόπο με τον οποίο οι χρήστες εργάζονται. Η λύσεις Citrix ενσωματώνουν επίσης λύσεις ασφαλείας τρίτων μερών για την μεγιστοποίηση του επιπέδου ασφαλείας.

2.3.1 Δυνατότητες ασφάλειας και συστάσεις για την ανάπτυξη περιβάλλοντος XenApp-XenDesktop

Οι πέντε πυλώνες ασφαλείας που προσφέρει η τεχνολογία Citrix είναι οι εξής: ταυτοποίηση και προσβασιμότητα, ασφάλεια δικτύου, ασφάλεια εφαρμογών, ασφάλεια δεδομένων, παρακολούθηση και αντιμετώπιση.

Η παραμετροποίηση των προϊόντων και χαρακτηριστικών Citrix σύμφωνα με τις απαιτήσεις του οργανισμού, ο σωστός σχεδιασμός και η συνεχής παρακολούθηση, ο έλεγχος και η αξιολόγηση της εγκατάστασης είναι καίρια σημεία για την διασφάλιση της μείωσης των απειλών ασφαλείας.

2.3.1.1 Ταυτοποίηση και Προσβασιμότητα

Για τον καθορισμό της ταυτοποίησης και προσβασιμότητας θα πρέπει να εξεταστούν οι απαιτήσεις του κάθε τύπου λογαριασμού καθώς ο καθένας παρουσιάζει διαφορετικές προκλήσεις και απαιτεί συγκεκριμένη ταυτοποίηση και διαμόρφωση πρόσβασης.

Για την ταυτοποίηση σε ένα ασφαλή περιβάλλον προτείνεται η πιστοποίηση “multi-factor authentication”, ένας συνδυασμός κωδικού ασφαλείας ακολουθούμενος από μία επιπλέον μέθοδο όπως hardware ή software-based token. Κάποιες επιπλέον μέθοδοι πιστοποίησης που υποστηρίζονται από το Citrix είναι οι ακόλουθες: Smartcards, Radius, Kerberos, Biometrics, ενώ σε απομακρυσμένου τύπου προσβάσεις η συγκεκριμένη μέθοδος τείνει να θεωρηθεί απαραίτητη. Η πιστοποίηση των χρηστών γίνεται μέσω του Storefront κυρίως εντός τοπικού δικτύου, ή μέσω Netscaler που προτείνεται για απομακρυσμένες προσβάσεις καθώς η σύνδεση εκτίθεται στο διαδίκτυο.

Πολύ σημαντική επίσης κρίνεται η επιβολή πολιτικών στους κωδικούς ασφαλείας έτσι ώστε να υπάρχουν κάποιες ελάχιστες απαιτήσεις όπως, ο κωδικός να αποτελείται από τουλάχιστον 8 χαρακτήρες και να περιέχει κάποιο κεφαλαίο και κάποιο ειδικό χαρακτήρα, ο κωδικός να λήγει ανά τακτά χρονικά διαστήματα αλλά και να μην επιτρέπεται η επαναχρησιμοποίηση παλιότερων κωδικών.

Τα δικαιώματα που δίδονται στους χρήστες διακρίνονται σε τρία επίπεδα, των *απλών χρηστών* όπου δίδονται τα ελάχιστα δικαιώματα που είναι απαραίτητα για την εκπλήρωση κάποιων εργασιών που καθορίζονται από τον οργανισμό και ανάλογα με τις ανάγκες χωρίζονται σε γκρουπ χρηστών στα οποία δίνονται κάποια επιπλέον δικαιώματα. Ο διαχωρισμός αυτός γίνεται μέσω του Active Directory του Domain Controller.
Των *διαχειριστών* "*administrators"* που απαιτούνται αυξημένα δικαιώματα για την διαχείριση κόνσολών, των δικαιωμάτων των απλών χρηστών και γενικότερα της υποδομής. Υπάρχουν πολλά διαφορετικά είδη λογαριασμών διαχειριστή στα οποία δίνονται διαφορετικού είδους προσβάσεις όπως για την διαχείριση των αποθηκευμένων δεδομένων, των βάσεων δεδομένων, της παρακολούθησης κόνσολών, την διαχείριση του XenApp και Xendesktop.
Των *υπηρεσιών* (service account), με αυξημένα προνόμια διαχείρισης όπου συνήθως γίνεται κακή διαχείριση κωδικών όπως για παράδειγμα η μη λήξη του κωδικού, η χρήση του ίδιου λογαριασμού για πολλαπλές υπηρεσίες. Οι λογαριασμοί αυτοί είναι συχνά στόχοι επιθέσεων, για αυτό το λόγο θα πρέπει να αποφεύγεται η κακή διαχείριση τους και να ισχύουν οι πολιτικές ορθής χρήσης των λογαριασμών που αναφέραμε παραπάνω.

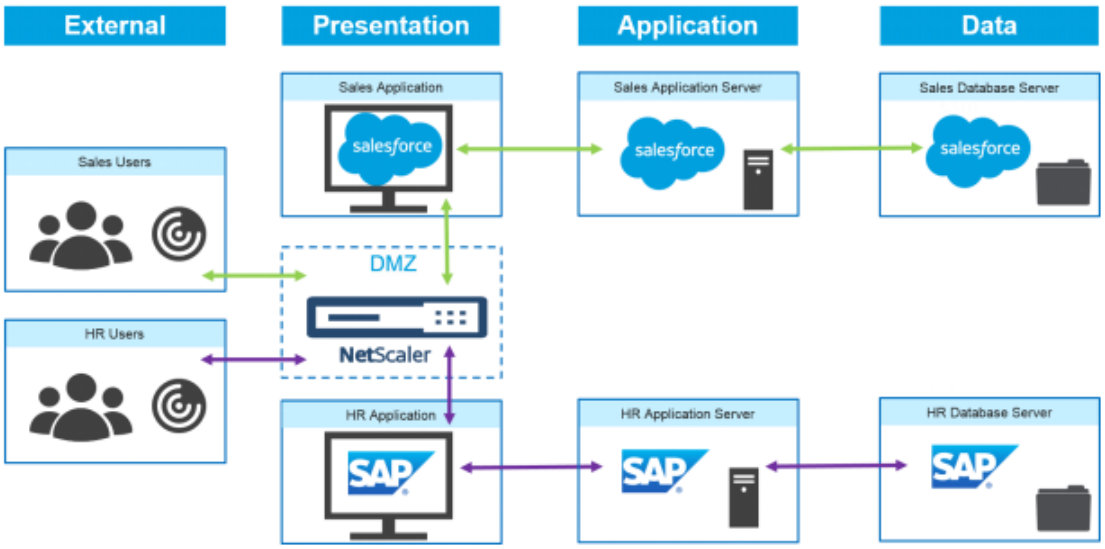
2.3.1.2 Ασφάλεια δικτύου

Ένα σωστά σχεδιασμένο δίκτυο με ασφαλή και διακριτά στρώματα βοηθά στην πρόληψη των παραβιάσεων ασφαλείας. Κάθε στρώμα είναι προστατευμένο και απομονωμένο ενώ η κυκλοφορία γίνεται μόνο μεταξύ γειτονικών στρωμάτων.
Τα firewalls χρησιμοποιούνται για την προστασία της κίνησης μεταξύ των στρωμάτων ενώ μόνο οι απαραίτητες πόρτες είναι ανοιχτές περιορίζοντας την κίνηση. Η κίνηση είναι κρυπτογραφημένη μεταξύ όλων των στρωμάτων.

Ένα παράδειγμα βλέπουμε παρακάτω όπου διακρίνονται τα διάφορα μέρη και οι πόροι της υποδομής στα στρώματα δικτύου:
External, το πιο ευπαθή μέρος του δικτύου, που δεν διαχειρίζεται από τον οργανισμό και είναι εκτεθειμένο στο διαδίκτυο.
Presentation, είναι διαχειρίσιμο από τον οργανισμό και περιέχει το Netscaler σε μία ζώνη DMZ από όπου δίδεται πρόσβαση σε εικονικές εφαρμογές και desktops.

Application, όπου αποτελείται από τους application-servers και τις κονσόλες διαχείρισης

Data, είναι το πιο προστατευμένο στρώμα στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα των χρηστών σε βάσεις δεδομένων και file-servers.



Εικόνα 2-3. Representative deployment

2.3.1.3 Ασφάλεια εφαρμογών

Η μεγαλύτερη απειλή σε αυτό το σημείο είναι η μέθοδος jealbreaking όπου μπορεί να προκύψει κακόβουλη δραστηριότητα, εκτέλεση κακόβουλου “unauthorized” λογισμικού, αφού αποκτηθεί πρόσβαση στην υποδομή του δικτύου.

Κάποια εργαλεία τρίτων μερών όπως το εργαλείο Microsoft Windows AppLocker συμβάλουν στην βελτίωση της ασφάλειας εφαρμογών, περιορίζοντας την πρόσβαση των χρηστών σε μία εφαρμογή αλλά και σε διαφορετικού τύπου αρχείων όπως εκτελέσιμα αρχεία και scripts.

Επίσης οι application και file-servers της υποδομής μπορούν να σχεδιαστούν ξεχωριστά και διακριτά μεταξύ τους στην υποδομή έτσι ώστε να παραμείνουν προστατευμένες οι εφαρμογές και τα δεδομένα, φυλασσόμενα σε διαφορετικούς servers και σημεία της υποδομής. Σε ευαίσθητες εφαρμογές θα πρέπει να επιβάλλονται υψηλότερα επίπεδα ασφάλειας για την πιστοποίηση των χρηστών όπως για παράδειγμα η μέθοδος multi-factor. Ένα επιπλέον μέτρο είναι η χρήση NTFS (New Technology File System) μέσω της οποίας περιορίζεται η πρόσβαση των χρηστών στους φακέλους των εφαρμογών.

2.3.1.4 Ασφάλεια δεδομένων

Το χαρακτηριστικό γνώρισμα της τεχνολογίας Citrix είναι ότι τα δεδομένα φιλοξενούνται στο data center έτσι η ασφάλεια τους στηρίζεται στο χαρακτηριστικό αυτό.

Εικονικά κανάλια (Virtual channels), θα πρέπει να προσδιορίζονται τα κανάλια που πρέπει να χρησιμοποιούνται και αυτά που πρέπει να παραμείνουν απενεργοποιημένα ανάλογα με τις ανάγκες των χρηστών σε αντιστοιχία με τις απαιτήσεις ασφαλείας που θέτει ο οργανισμός. Θα πρέπει να περιορίζεται η χρήση των καναλιών όπου αυτό είναι εφικτό, όπως για παράδειγμα στην χαρτογράφηση των δίσκων του χρήστη (drive mapping) ή των συσκευών USB (USB redirection) όπου επιτρέπεται η μεταφορά δεδομένων μεταξύ των τελικών συσκευών των χρηστών και του data center.
Σε περιπτώσεις όπου διαφέρουν οι απαιτήσεις για τους χρήστες του τοπικού δικτύου και των απομακρυσμένων χρηστών, οι ρυθμίσεις των εικονικών καναλιών μπορεί να είναι διαχειρίσιμες μέσω της διαμόρφωσης της μεθόδου πρόσβασης Smartaccess, έτσι οι ρυθμίσεις βασίζονται ανάλογα με την προσβασιμότητα του χρήστη στο περιβάλλον μέσω τοπικού δικτύου-intranet ή απομακρυσμένης πρόσβασης.
Σε γενικές γραμμές η ενεργοποίηση εικονικών καναλιών θα πρέπει να συμβαίνει όταν αυτά είναι απολύτως απαραίτητα για την παραγωγικότητα των χρηστών που τα χρησιμοποιούν και αν ο κίνδυνος σε επίπεδο ασφάλειας που προκύπτει είναι αποδεκτός από τον οργανισμό.

Netscaler Gateway, η δικτυακή πύλη του Netscaler μπορεί να ρυθμιστεί έτσι ώστε να χρησιμοποιείται η λειτουργία ICA proxy, εξασφαλίζοντας την διαθεσιμότητα των δεδομένων μόνο μέσω δημοσιευμένων εφαρμογών και desktops και όχι άμεσης διαθεσιμότητας ακόμα και για προσβάσεις μέσω του τοπικού δικτύου.

Ευαίσθητα δεδομένα, η πρόσβαση σε τέτοιου είδους δεδομένα απαιτεί υψηλότερα επίπεδα ασφάλειας στον έλεγχο της ταυτότητας του χρήστη, έτσι σε ένα περιβάλλον που εμπεριέχει κρίσιμες πληροφορίες η χρήση επιπλέον μεθόδου ταυτοποίησης όπως smartcards ή token κρίνεται απαραίτητη.

Provisioning: ανάλογα με την διάθεση των υπηρεσιών μπορεί να αυξηθούν ή αντιθέτως να μειωθούν οι πιθανότητες παραβιάσεων ασφαλείας. Για παράδειγμα σε περίπτωση που δίδεται ένα virtual desktop στον χρήστη σε λειτουργία “read-only” στο τέλος της σύνδεσης το desktop απορρίπτεται, έτσι σε περίπτωση παραβίασης ασφαλείας η απειλή μετριάζεται κατά την λήξη της σύνδεσης.

Φιλοξενία εφαρμογών και δεδομένων, θα πρέπει να διασφαλιστεί η φύλαξη των δεδομένων και των εφαρμογών σε κατάλληλα σημεία και τοποθεσίες, έτσι θα πρέπει

να αποκλειστεί η ύπαρξη και δυνατότητα αναπαραγωγής εκτελέσιμων αρχείων και scripts σε servers όπου φιλοξενούνται δεδομένα, επίσης θα πρέπει να ισχύει η απαγόρευση πρόσβασης και τροποποίησης αρχείων από τους χρήστες σε servers όπου φιλοξενούνται εφαρμογές.

2.3.1.5 Παρακολούθηση και Αντιμετώπιση

Η παρακολούθηση “Monitoring” είναι απαραίτητη για τον εντοπισμό και την αντιμετώπιση των κινδύνων ασφαλείας, επιτρέποντας την βελτιστοποίηση της ασφάλειας και της συμμόρφωσης. Βασίζεται στην ανίχνευση και αντιμετώπιση ύποπτων δραστηριοτήτων και επιθέσεων, ανίχνευση κατάχρησης των δικαιωμάτων που έχει ένας χρήστης προνομιακού λογαριασμού, διασφάλιση πως όλα τα προϊόντα είναι ενημερωμένα με τις τελευταίες επιδιορθώσεις ασφαλείας “patches” όπως και το λογισμικό προστασίας είναι ενημερωμένο και εγκατεστημένο.

Ένας οργανισμός είναι απαραίτητο να εξετάσει την στρατηγική που θα ακολουθήσει για τους κινδύνους που εγκυμονούν ως προς τον εντοπισμό, την αποτροπή, την πρόληψη και την ανάκαμψη από αυτούς.

Εντοπισμός: μπορεί να προέλθει μέσω της παρακολούθησης, όπως για παράδειγμα με την χρήση του χαρακτηριστικού του Netscaler “security insight” που οδηγεί στον εντοπισμό ζητημάτων συμμόρφωσης και ευαίσθητων σημείων στις αναφορές που προκύπτουν από τα αρχεία καταγραφής που προέρχονται από τον Netscaler.

Αποτροπή: η παρακολούθηση της συμπεριφοράς χρηστών δεν βοηθά απλά στον εντοπισμό ζητημάτων ασφαλείας αλλά και στην αποτροπή της κακόβουλης δραστηριότητας χρηστών όταν αυτοί γνωρίζουν πως οι πέραν του φυσιολογικού δραστηριότητες τους παρακολουθούνται.

Πρόληψη: τεχνικές όπως κατάτμηση των χρηστών, των εφαρμογών και των δεδομένων, η πρόσβαση σε εφαρμογές και δεδομένα βάση πολιτικών ασφαλείας καθώς και η αποφυγή αποθήκευσης δεδομένων σε απομακρυσμένες συσκευές εκτός οργανισμού μπορούν να βοηθήσουν στην πρόληψη των κινδύνων. Επίσης η σωστή εκπαίδευση των χρηστών είναι ένα στοιχείο στο οποίο πολλοί οργανισμοί δεν επενδύουν όμως μπορεί να βοηθήσει σε μεγάλο σημείο.

Ανάκτηση: οι εικονικές εφαρμογές και desktops παρέχουν χαρακτηριστικά που βοηθούν στην ανάκτηση και αντιμετώπιση ζητημάτων ασφαλείας. Σε περίπτωση που εντοπιστεί κάποια παραβίαση ασφαλείας μπορεί να αναδιαμορφωθεί η ανάπτυξη της υποδομής και να επανεξεταστούν οι όποιες διαδικασίες ακολουθήθηκαν για την πρόληψη άλλων παρόμοιων απειλών.

Οι απαιτήσεις συμμόρφωσης θα πρέπει να εξεταστούν ενδελεχώς από έναν οργανισμό και πάντα σύμφωνα με τις ανάγκες που προκύπτουν. Η κατάλληλη

κρυπτογράφηση, η κατάτμηση των χρηστών και της πρόσβασης αυτών στους πόρους της υποδομής, η διαχείριση των δεδομένων, είναι σημαντικοί παράγοντες στην παροχή μιας συνεπούς συμμόρφωσης ασφαλείας.

2.3.2 Πρότυπα ασφαλείας

Σε αυτήν την ενότητα παρουσιάζονται τα πρότυπα ασφαλείας που πρέπει να εφαρμοστούν για να οδηγήσουν την ασφάλεια της υποδομής Citrix σε υψηλά επίπεδα. Κάποια από αυτά είναι απαραίτητο να εφαρμοστούν ανάλογα με την κάθε περίπτωση και τις ανάγκες της επιχείρησης.

2.3.2.1 Common Criteria Certification

Ένα διεθνώς αναγνωρισμένο πρότυπο για την αξιολόγηση της ασφάλειας των προϊόντων και συστημάτων πληροφορικής, παρέχει την διασφάλιση ότι τα προϊόντα έχουν δοκιμαστεί διεξοδικά και ανεξάρτητα και έχουν επικυρωθεί από μία σειρά απαιτήσεων που καθορίζονται από την διεθνή οργάνωση προτύπων για την διασφάλιση της ασφάλειας στον τομέα της πληροφορικής.
Για τους διεθνής κυβερνητικούς οργανισμούς όπως και για τους τομείς της υγειονομικής περίθαλψης και οικονομίας είναι απολύτως απαραίτητη η εφαρμογή του προτύπου για την σύναψη έργων πληροφοριακού περιεχομένου.

Η τεχνολογία Citrix καλύπτει σε όλες τις πλατφόρμες της αυτά τα πρότυπα, για παράδειγμα η πλατφόρμα XenDesktop, XenApp 7.6 και Netscaler 10.5 αξιολογήθηκαν σύμφωνα με τα πρότυπα UK IT Security Evaluation και Certification Scheme και πληρούν τις απαιτήσεις του προτύπου.

2.3.2.2 FIPS 140-2

Το πρότυπο “Federal Information Processing Standard 140” της ομοσπονδιακής κυβέρνησης των ΗΠΑ που καθορίζει ένα σημείο αναφοράς για την εφαρμογή κρυπτογράφησης λογισμικού. Παρέχει τις βέλτιστες πρακτικές για την χρήση κρυπτογραφικών αλγόριθμων και την αλληλεπίδραση με το λειτουργικό σύστημα.

Η πρώτη έκδοση του προτύπου εκδόθηκε το 1994 “FIPS 140-1” όπου καθιερώθηκαν οι απαιτήσεις κρυπτογραφίας παρέχοντας τέσσερα επίπεδα ασφαλείας , επιτρέποντας έτσι οικονομικές και αποδοτικές λύσεις κατάλληλες για τις διαφορετικές ανάγκες των οργανισμών.
Το 2002 αντικαταστάθηκε από το “FIPS 140-2” στο οποίο ενσωματώθηκαν οι αλλαγές στα πρότυπα και στην τεχνολογία, ενώ το “FIPS 140-3” (2004) είναι η τελευταία έκδοση που ισχύει μέχρι και σήμερα και περιλαμβάνει ένα επιπλέον επίπεδο ασφαλείας στο οποίο ενσωματώνονται νέα χαρακτηριστικά που αντικατοπτρίζουν τις εξελίξεις στην τεχνολογία των ημερών μας.

Για την εκπλήρωση των απαιτήσεων του προτύπου FIPS τα προϊόντα Citrix χρησιμοποιούν κρυπτογραφικές μονάδες επικυρωμένες από τα λειτουργικά Microsoft Windows “Microsoft Cryptography Application Programming Interface (CryptoAPI)” εφαρμόζοντας ασφαλείς συνδέσεις TLS και SSL στα παρακάτω μέρη τους:

- XenApp
- Citrix Receiver and Citrix online plug-in
- Web Interface
- SSL Relay
- Secure Gateway for Windows
- Single Sign-on
- Offline applications (streaming)
- SmartAuditor
- Power and Capacity Management
- Configuration Logging
- ICA File Signing

Τα μέρη αυτά της τεχνολογίας Citrix θα πρέπει να λειτουργούν με συμβατό τρόπο ως προς το πρότυπο FIPS, ειδικά αυτά που χρησιμοποιούν TLS θα πρέπει να ρυθμιστούν για να χρησιμοποιούν πακέτα αλγόριθμων κρυπτογράφησης όπως:

- RSA_WITH_3DES_EDE_CBC_SHA [RFC 2246]
- RSA_WITH_AES_128_CBC_SHA [FIPS 197, RFC 3268]
- RSA_WITH_AES_256_CBC_SHA [FIPS 197, RFC 3268]

2.3.2.3 Πρωτόκολλα TLS/SSL

Το πρωτόκολλο TLS “Transport Layer Security” προήλθε από την εξέλιξη του SSL “Secure Sockets Layer” το 1995, ενώ με τις διαδοχικές εκδόσεις του πρωτοκόλλου έχουν προστεθεί:

- ✓ Διορθωτικές αλλαγές στις αδυναμίες των παλαιότερων εκδόσεων
- ✓ Υποστήριξη των νέων κρυπτογραφικών αλγορίθμων και νέα χαρακτηριστικά στο πρωτόκολλο

Στην τεχνολογία Citrix υπάρχει η δυνατότητα ενεργοποίησης του πρωτοκόλλου TLS για την ασφαλή επικοινωνία μεταξύ των συσκευών του χρήστη και των Citrix-servers.

Η κρυπτογραφία στο πρωτόκολλο TLS ορίζεται από μία ακολουθία κρυπτογράφησης, που γίνεται αντικείμενο διαπραγμάτευσης μεταξύ του server και του client και ορίζει τον κρυπτογραφικό αλγόριθμο που θα χρησιμοποιηθεί. Κάποιοι από τους αλγόριθμους αυτούς θεωρούνται αδύναμοι και έτσι τα προϊόντα Citrix αποτρέπουν αυτόματα την χρήση τους ή είναι απενεργοποιημένοι από προεπιλογή.

Ένα παράδειγμα ακολουθίας κρυπτογράφησης είναι το ακόλουθο:
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Και ερμηνεύεται ως εξής:
TLS (Transport Layer Security) είναι το πρωτόκολλο ασφαλείας

ECDHE_RSA (Elliptic Curve Diffe-Hellman) είναι ο αλγόριθμος που χρησιμοποιείται για την ανταλλαγή κλειδιού, ενώ ένα πιστοποιητικό RSA είναι απαραίτητο να χρησιμοποιηθεί

AES_256_CBC (Advanced Encryption Standard, Cipher Block Chaining) είναι η μέθοδος κρυπτογράφησης όπου χρησιμοποιείται ένα κλειδί 256-bit

SHA384 (Secure Hash Algorithm) ο κωδικός αυθεντικότητας του μηνύματος (MAC)

Υπάρχουν κάποιες ακολουθίες κρυπτογράφησης που θεωρούνται αδύναμες και αυτό σημαίνει ότι υπάρχει δυνατότητα επιτυχούς επίθεσης ή είναι πιθανό να προκύψει κάποια τέτοια στα επόμενα χρόνια με τον ρυθμό ανάπτυξης της τεχνολογίας που υπάρχει σήμερα. Για αυτό το λόγο θα πρέπει να επαληθεύεται περιοδικά η αντοχή των κρυπτογραφικών αλγορίθμων μέσω αξιόπιστων και διεθνώς αναγνωρισμένων πηγών.

Ανάμεσα στους αλγόριθμους που θεωρούνται αδύναμοι είναι αυτοί που φαίνονται στον παρακάτω πίνακα.

Algorithm	In certificates	In ciphersuites
DES	–	Weak
RC2	–	Weak
RC4	–	Weak
3DES (TDEA)	–	Not weak
MD2	Weak	–
MD5	Weak	Not weak, but avoid
SHA1	Weak	Not weak

Πίνακας 2-2. Αδύναμοι Αλγόριθμοι

Οι αλγόριθμοι οι οποίοι προτείνονται σήμερα και είναι κατά βάση πιο ισχυροί είναι οι εξής:

- AES-CBC (Cipher Block Chaining)
- AES-CCM (Counter with Cipher Block Chaining-Message Authentication Code)
- AES-GCM (Galois Counter Mode)

Ο CCM σπάνια χρησιμοποιείται ενώ ο GCM προτιμάται από τον CBC καθώς έχει καλύτερη απόδοση και είναι ανθεκτικός σε επιθέσεις side-channel και plaintext.

Οι εκδόσεις TLS είναι οι εξής:

TLS 1.0, υποστηρίζεται ευρέως όπως και σε προϊόντα Citrix και είναι ευπαθή σε επιθέσεις BEAST (Browser Exploit Against SSL/TLS), για αυτό το λόγο δεν προτείνεται η εφαρμογή του σε υλοποιήσεις νέων προϊόντων.

TLS 1.1, είναι λιγότερο διαδεδομένο καθώς γρήγορα αντικαταστάθηκε από το TLS 1.2 και δεν είναι ευπαθή σε επιθέσεις BEAST όπως και η επόμενη έκδοση.

TLS 1.2, είναι η προτιμότερη έκδοση για νέες υλοποιήσεις και εμπεριέχει τις νεότερες κρυπτογραφικές ακολουθίες όπως SHA256, SHA384. Συνίσταται και απαιτείται ακόμα από διάφορους διεθνής κανονισμούς.

2.3.2.4 IP Security

Είναι μια επέκταση του πρωτοκόλλου IP που παρέχει επικυρωμένη και κρυπτογραφημένη επικοινωνία με ακεραιότητα δεδομένων. Είναι ένα πρωτόκολλο που εφαρμόζεται σε επίπεδο δικτύου, έτσι πρωτόκολλα που εφαρμόζονται σε υψηλότερο επίπεδο (όπως το Citrix ICA) μπορούν να το χρησιμοποιήσουν χωρίς τροποποίηση. Οι παλαιότερες εκδόσεις XenApp και XenDesktop ήταν απαραίτητο να χρησιμοποιούν το πρωτόκολλο IPSec αλλά στις τελευταίες εκδόσεις που χρησιμοποιείται end-to-end κρυπτογράφηση μέσω πρωτοκόλλου TLS δεν είναι απαραίτητη η χρήση του.

2.3.2.5 Smart Cards

Η χρήση έξυπνων καρτών είναι δυνατή στα προϊόντα Citrix και μέσω αυτών παρέχεται ασφαλής πρόσβαση σε υπολογιστικούς πόρους και δεδομένα, με τον τρόπο αυτό απλοποιείται η διαδικασία πρόσβασης ενώ παράλληλα ενισχύεται και η ασφάλεια. Ο χρήστης μπορεί να έχει πρόσβαση μέσω της κάρτας σε μία δημοσιευμένη εφαρμογή Citrix, όπως για παράδειγμα η εφαρμογή Microsoft Outlook. Στο δίκτυο μιας επιχείρησης οι έξυπνες κάρτες αποτελούν μια αποτελεσματική εφαρμογή του δημόσιου κλειδιού και μπορεί να χρησιμοποιηθεί για:

- Πιστοποίηση των χρηστών σε δίκτυα και συσκευές
- Επικοινωνίες ασφαλών καναλιών πάνω σε ένα δίκτυο
- Χρήση ψηφιακών υπογραφών για την εξασφάλιση του περιεχομένου

Πέρα από την ασφαλή ταυτοποίηση των χρηστών για την χρήση μιας εφαρμογής, η έξυπνη κάρτα μπορεί να υποστηρίζεται και από την ίδια την εφαρμογή, έτσι για παράδειγμα μπορεί ο χρήστης να ταυτοποιηθεί για την χρήση της εφαρμογής Microsoft Outlook αλλά και να χρησιμοποιήσει το πιστοποιητικό που εμπεριέχεται στην κάρτα έτσι ώστε να υπογράψει ψηφιακά ένα mail που θα αποστείλει.

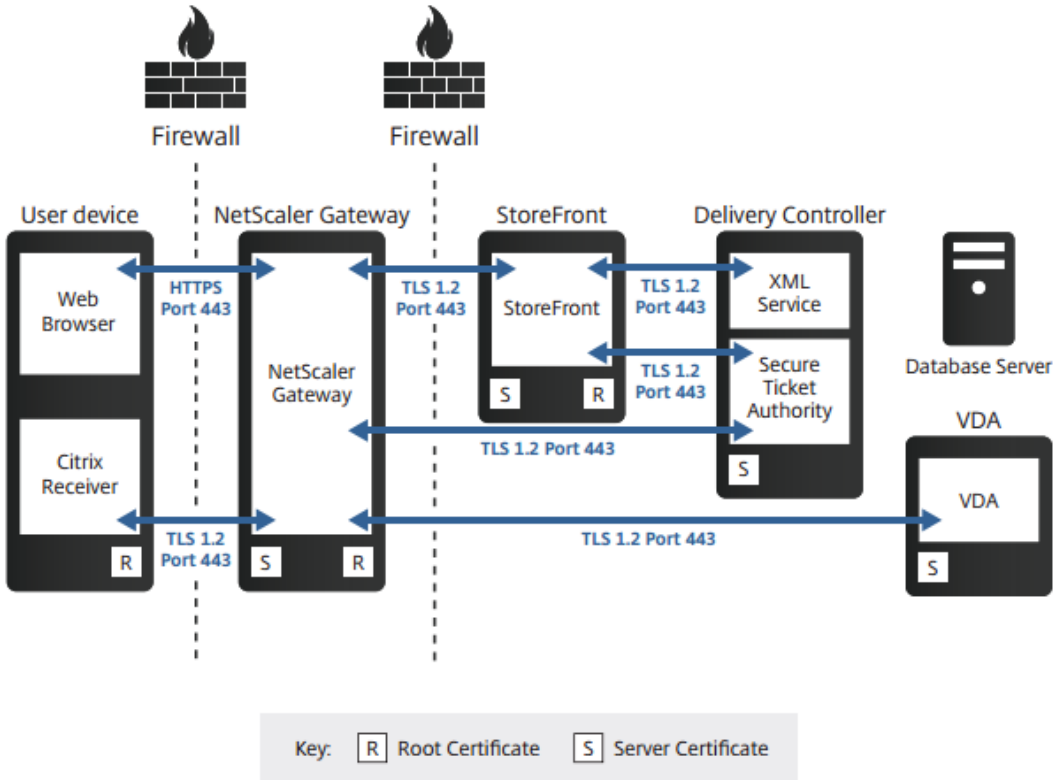
Η τεχνολογία Citrix υποστηρίζει την χρήση προσωπικών υπολογιστών που βασίζονται στην χρήση έξυπνων καρτών οι οποίες υποστηρίζουν λειτουργίες όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές. Οι κάρτες κρυπτογραφίας είναι σχεδιασμένες για την ασφαλή αποθήκευση ιδιωτικών κλειδιών όπως αυτά που χρησιμοποιούνται σε συστήματα ασφαλείας PKI (Public Key Infrastructure). Οι λειτουργίες κρυπτογραφίας γίνονται εξολοκλήρου μέσα στην κάρτα με αποτέλεσμα να μην γίνεται η χρήση των ιδιωτικών κλειδιών και πιστοποιητικών εκτός της κάρτας όπου θα ήταν πιθανή η υποκλοπή τους.

Για την βελτιστοποίηση της ασφάλειας προτείνεται η χρήση του ελέγχου ταυτότητας “two factor” που σημαίνει ότι πέρα από την χρήση της έξυπνης κάρτας (one factor) μπορεί να χρησιμοποιηθεί επιπρόσθετα και ένας προσωπικός κωδικός (two factor) που είναι γνωστός μόνο στον χρήστη και πιστοποιεί πως είναι ο νόμιμος ιδιοκτήτης της κάρτας.

2.3.3 Αντιπροσωπευτική ανάπτυξη XenApp-XenDesktop

Για την ανάπτυξη μιας ασφαλούς υποδομής, το περιβάλλον Citrix θα πρέπει να σχεδιαστεί έτσι ώστε να καλύπτει κάποια από τα απαραίτητα χαρακτηριστικά ασφαλείας που αναφέρονται παραπάνω. Ο σχεδιασμός που περιγράφεται στην παρακάτω εικόνα είναι ένα χαρακτηριστικό παράδειγμα που περιλαμβάνει, Citrix receiver, Netscaler gateway, Storefront, XenApp και XenDesktop (Delivery Controller και VDA).

Πιο συγκεκριμένα χρησιμοποιείται Storefront 3.5 καθώς στην συγκεκριμένη έκδοση υποστηρίζεται η κρυπτογράφηση της δικτυακής κίνησης μέσω TLS 1.2 πρωτοκόλλου, όπως επίσης και Netscaler Gateway MPX 11.0 όπου με την εφαρμογή του firmware 2.2 level cavium επιτρέπει επίσης την χρήση TLS 1.2.



Εικόνα 2-4. Αντιπροσωπευτική ανάπτυξη XenApp-XenDesktop

Οι χρήστες συνδέονται στον Netscaler, ο οποίος βρίσκεται εντός της περιοχής DMZ, όπου γίνεται η ταυτοποίηση μέσω της μεθόδου “two factor”.

Ανάλογα με τα δικαιώματα του χρήστη είναι διαθέσιμες σε αυτόν συγκεκριμένες εφαρμογές και υπολογιστικοί πόροι.
Οι εφαρμογές και τα δεδομένα είναι αποθηκευμένα σε κατάλληλες τοποθεσίες και διαχωρισμένους servers έτσι ώστε να παραμένουν ασφαλή τα ευαίσθητα δεδομένα και οι εφαρμογές.
Η ανάπτυξη περιλαμβάνει προγράμματα παρακολούθησης για τον έλεγχο των χρηστών και τα θέματα ασφαλείας που μπορούν να προκύψουν.
Αναλυτικότερα διακρίνουμε τα πιστοποιητικά του κάθε server αλλά και το πρωτόκολλο ασφαλείας και τις πόρτες που χρησιμοποιούνται.
Η κίνηση μεταξύ του web browser που χρησιμοποιεί ο χρήστης στην συσκευή του και του Netscaler γίνεται με την χρήση του πρωτοκόλλου ασφαλείας HTTPS και του TLS 1.2.
Στον Netscaler τερματίζει η σύνδεση TLS/HTTPS από τον web browser και τον Citrix receiver που βρίσκονται στην συσκευή του τελικού χρήστη. Από εκεί και έπειτα η κίνηση προς τον Storefront, Delivery controller και VDA ασφαλίζεται κάνοντας χρήση TLS 1.2.
Η δικτυακή κίνηση είναι κρυπτογραφημένη σε όλη τη διάρκεια της και σε όλα τα σημεία “end to end encryption” μέσω TLS 1.2, καθώς όλα τα μέρη της συγκεκριμένης ανάπτυξης μπορούν να υποστηρίξουν το πρωτόκολλο TLS 1.2.

3 Citrix Netscaler ADC

Το σημαντικότερο μέρος για την ασφάλεια της υποδομής Citrix είναι ο Netscaler Application Delivery Controller (ADC) που με τις κατάλληλες ρυθμίσεις και τα χαρακτηριστικά που προσδίδει μπορεί να παρέχει αποτελεσματική προστασία από πολλές επιθέσεις όπως DDoS, SQL injection, XSS, SSL-based. Πέραν όμως της ασφάλειας, παρέχει επίσης βελτίωση της απόδοσης και ενίσχυση της διαθεσιμότητας των εφαρμογών μέσω του χαρακτηριστικού της εξισορρόπησης φορτίου “load balancing” που διαθέτει.

3.1 Μοντέλα και εκδόσεις του Citrix Netscaler

Ο Citrix Netscaler διακρίνεται στα παρακάτω προϊόντα:

Netscaler MPX, ένα hardware-based ποιόν με απόδοση 500 Mbps – 160 Gbps το οποίο είναι κατάλληλο για διαχείριση εφαρμογών web-based κίνησης πολλών Gigabits. Διαθέτει την δυνατότητα εξισορρόπησης φορτίου (load balancing) ενώ αυξάνει την ασφάλεια στις εφαρμογές που διαχειρίζεται.

Netscaler SDX, είναι επίσης ένα προϊόν hardware-based με αυξημένες δυνατότητες δημιουργίας εικονικού περιβάλλοντος (virtualization), έχοντας τη δυνατότητα φιλοξενίας 115 ανεξάρτητων οντοτήτων Netscaler. Αποδίδοντας έως και 160 Gbps μπορεί να υποστηρίξει την ενοποίηση μεγάλων υπολογιστικών υποδομών καθώς και την παροχή πολλαπλής μίσθωσης για οργανισμούς διατηρώντας παράλληλα την απομόνωση της υποδομής κάθε οργανισμού χωρίς περιορισμούς. Γνωρίζοντας τα παραπάνω είναι προφανές ότι το συγκεκριμένο προϊόν ενδείκνυται για την χρήση του σε cloud-based υποδομές.

Netscaler VPX, εικονικές συσκευές software-based οι οποίες αναπτύσσονται σε hypervisors αποδίδοντας 10 Mbps – 40 Gbps. Κατάλληλο προϊόν για cloud υποδομές που δίνει τη δυνατότητα πολλαπλής μίσθωσης, μπορεί να χρησιμοποιηθεί ευκολότερα σε μη παραγωγικά περιβάλλοντα και επίσης είναι μια ελκυστική, χαμηλού κόστους επιλογή, που ανταποκρίνεται στις ανάγκες μικρότερων οργανισμών.

Netscaler CPX, πλαισιώνει τις προηγούμενες κατηγορίες ως ένα cloud-ready προϊόν κατάλληλο για ομάδες προγραμματιστών και διαχείριση δικτύου καθώς είναι σχεδιασμένο να λειτουργεί στα αρχικά στάδια ανάπτυξης μιας εφαρμογής παρέχοντας την δυνατότητα εξισορρόπησης φορτίου στην αρχή του κύκλου ανάπτυξης της εφαρμογής.

Οι εκδόσεις του Netscaler χωρίζονται στις παρακάτω κατηγορίες:

Standard edition, παρέχει σε μικρούς και μεσαίους οργανισμούς διαχείριση δικτυακής κυκλοφορίας επιπέδου 4-7 αυξάνοντας την διαθεσιμότητα των web-based εφαρμογών.

Enterprise edition, αυξάνει τις επιδόσεις και την διαθεσιμότητα των εφαρμογών διαχειρίζοντας με προηγμένα μέσα την δικτυακή κυκλοφορία, μειώνοντας παράλληλα το κόστος των data-centers.

Platinum edition, εμπεριέχει τις δυνατότητες των παραπάνω, όπως επίσης την δυνατότητα παρακολούθησης της απόδοσης των εφαρμογών αλλά και της προηγμένης ασφάλειας αυτών.

Στον παρακάτω πίνακα βλέπουμε αναλυτικά τα χαρακτηριστικά της κάθε έκδοσης.

Feature	Platinum Edition	Enterprise Edition	Standard Edition
Application availability			
L4 load balancing and L7 content switching	●	●	●
Database load balancing[1]	●	●	●
AppExpert rate controls	●	●	●
IPv6 support	●	●	●
Traffic domains	●	●	●
Global server load balancing (GSLB)	●	●	○
Dynamic routing protocols	●	●	
Surge protection and priority queuing	●	●	
TriScale clustering	○	○	○
Application acceleration			
Client and server TCP optimizations	●	●	●
Citrix AppCompress for HTTP	●	●	○
Citrix AppCache	●	○	
NetScaler CloudConnectors	○	○	○
Citrix Branch Repeater client	●		
Application security			
L4 DoS defenses	●	●	●
L7 content filtering and HTTP/URL rewrite	●	●	●
NetScaler Gateway, SSL VPN	●	●	●
XenMobile NetScaler Connector	●	●	●
SAML2 support	●	●	●
L7 DoS defenses	●	●	
AAA for traffic management	●	●	
Citrix Application Firewall with XML security	●	○	
NetScaler CloudBridge Connector	●		
Simple manageability			
NetScaler Insight Center	●	●	●
AppExpert visual policy builder	●	●	●
ActionAnalytics	●	●	●
AppExpert service callouts, templates and Visualizers	●	●	●
Role-based administration and AAA for administration	●	●	●
Configuration wizards	●	●	●
Native Citrix Web Interface	●	●	●
Citrix Command Center	●	●	
Citrix EdgeSight for NetScaler	●	○	
Web 2.0 optimization			
Rich Internet application support and XML XPath support	●	●	●
Advanced server offload	●	●	
Lower TCO			
TCP buffering	●	●	●
TCP and SQL multiplexing	●	●	●
SSL offload and acceleration	●	●	●
Cache redirection including multi-layer support	●	●	

● Standard ○ Option

Πίνακας 3-1. Netscaler Editions

3.2 Τοπολογία δικτύου και λειτουργικά χαρακτηριστικά

Ένα πολύ σημαντικό κομμάτι για την κατανόηση της λειτουργίας του Netscaler είναι ο τρόπος επικοινωνίας του με τους clients και servers αλλά και η θέση του στο δίκτυο, η οποία μπορεί να ποικίλει καθώς όπως θα δούμε παρακάτω υπάρχουν αρκετά διαφορετικά σενάρια τοπολογιών που το κάθε ένα αναδεικνύει τα πολλά πλεονεκτήματα του προϊόντος.

3.2.1 Σε ποια θέση του δικτύου βρίσκεται ο Netscaler

Ο Netscaler είναι η ενδιάμεση οντότητα μεταξύ των clients και των servers, έτσι όλες οι αιτήσεις των clients διέρχονται από αυτόν. Σε μία τυπική εγκατάσταση ο Netscaler παρέχει public IPs σε κάθε εικονικό εξυπηρετητή (virtual server) οι οποίες χρησιμοποιούνται από τους clients για να αποκτήσουν πρόσβαση στις εφαρμογές που βρίσκονται εγκατεστημένες στους servers. Οι φυσικοί servers στους οποίους φιλοξενείται το εικονικό αυτό περιβάλλον βρίσκονται σε ένα απομονωμένο-ιδιωτικό δίκτυο. Υπάρχει επιπλέον η δυνατότητα χρησιμοποίησης της συσκευής Netscaler σε επίπεδο (OSI model) L2 (bridge) ή L3 (Router) και σε συνδυασμό αυτών.

Λειτουργία σε επίπεδο L2

Σε αυτό το επίπεδο ο Netscaler προωθεί πακέτα μεταξύ διασυνδέσεων δικτύου (network interfaces) όταν ισχύουν οι παρακάτω παράμετροι:

- Τα πακέτα προορίζονται για την διεύθυνση MAC μιας άλλης συσκευής
- Η διεύθυνση αυτή βρίσκεται σε ένα διαφορετικό network interface
- Το network interface είναι μέλος του ίδιου Virtual LAN

Από προεπιλογή όλα τα network interfaces είναι μέλη ενός προκαθορισμένου VLAN, τα αιτήματα και οι απαντήσεις που διακινούνται μέσω του πρωτοκόλλου ARP (Address Resolution Protocol) διαβιβάζονται σε όλα τα μέλη. Σε περίπτωση λειτουργίας και δεύτερης συσκευής ως L2 παρατηρούνται “bridging loops” και πρέπει να αποφευχθεί για τη σωστή λειτουργία του δικτύου.

Λειτουργία προώθησης πακέτων L3

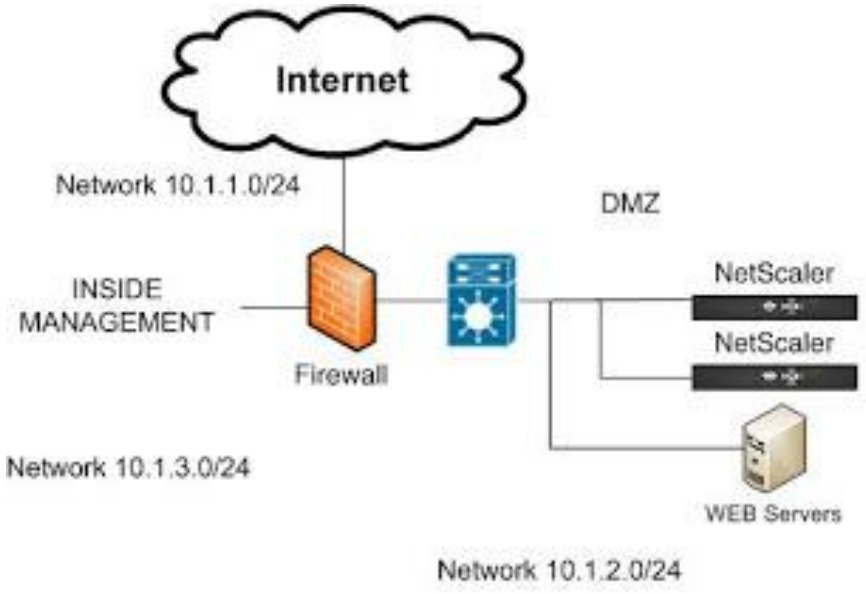
Κατά αυτή τη λειτουργία ο Netscaler προωθεί πακέτα έχοντας ως προοσισμό μία IP διεύθυνση που δεν είναι διαμορφωμένη εσωτερικά αλλά υπάρχει μία διαδρομή προς τον προορισμό στον πίνακα δρομολόγησης του Netscaler (routing table), λειτουργεί δηλαδή ως ένας δρομολογητής (router). Ο Netscaler, σε όποια λειτουργία και αν βρίσκεται, απορρίπτει πακέτα που διαθέτουν τα παρακάτω χαρακτηριστικά:

- Πλαίσια πολλαπλής διανομής (multicast frames)

- Άγνωστα πλαίσια πρωτοκόλλου που προορίζονται στη MAC διεύθυνση του Netscaler
- Πακέτα που μεταφέρονται μέσω πρωτοκόλλου “spanning tree”

3.2.2 Τοπολογία One-arm και Two-arm

Στην τοπολογία *one-arm* μόνο ένα network interface είναι συνδεδεμένο σε ένα τμήμα δικτύου Ethernet, σε αυτήν την περίπτωση δεν απομονώνονται οι δύο πλευρές client-server του δικτύου. Στο παρακάτω παράδειγμα μπορούμε να δούμε την ακριβή του θέση που βρίσκεται εντός της περιοχής DMZ του δικτύου, στο ίδιο subnet με τους web-servers.



Εικόνα 3-1. Τοπολογία One-Arm

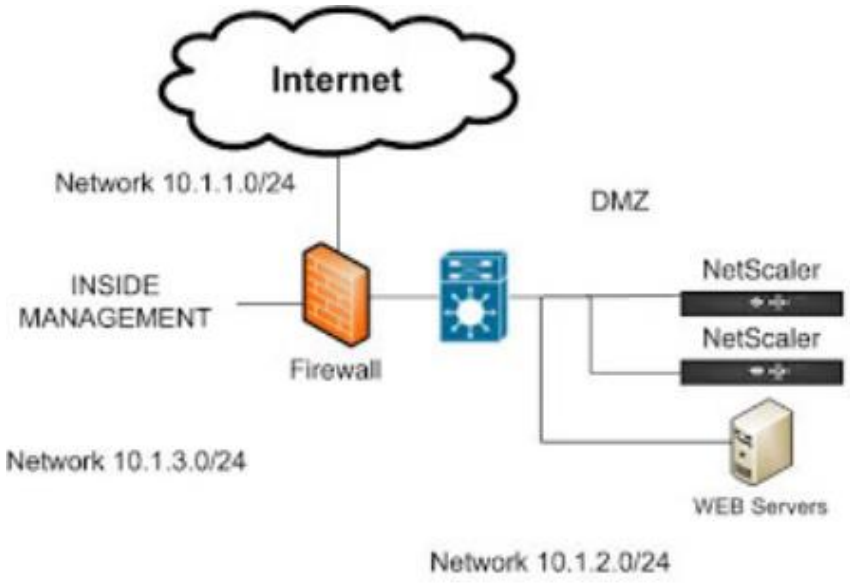
Το πλεονέκτημα αυτής της περίπτωσης είναι η ευκολία υλοποίησης, λόγω απλοποίησης της διαδικασίας δρομολόγησης, χωρίς όμως αυτό να σημαίνει ότι αυτός είναι σε κάθε περίπτωση ο σωστός τρόπος.

Σε περίπτωση που οι servers διαθέτουν δημόσιες IPs θα πρέπει να ακολουθηθεί η διαδικασία NAT (Network Address Translation) στο firewall για την σωστή δρομολόγηση των πακέτων.

Ένα ακόμα ζήτημα που προκύπτει σε αυτήν την τοπολογία είναι κατά την λειτουργία εξισορρόπησης φορτίου του Netscaler στο εσωτερικό δίκτυο (π.χ. δίνοντας πρόσβαση μέσω δημόσιας IP σε κάποιο Sharepoint site ή σε ένα Web interface) ενώ παράλληλα χρησιμοποιείται πρόσβαση SSL VPN, όπου σε αυτήν την περίπτωση θα πρέπει να δημιουργηθούν κανόνες στο firewall. Εδώ προκύπτει ζήτημα ασφαλείας καθώς οι Web servers, όπως δείχνει και η παραπάνω εικόνα, δεν βρίσκονται προστατευόμενοι πίσω από τον Netscaler αλλά στην ίδια DMZ περιοχή. Αυτό το

ζήτημα μπορεί να εξαλειφθεί με τους σωστούς περιορισμούς που μπορεί να επιβάλει ο διαχειριστής του δικτύου στο firewall αλλά ακόμα περισσότερο με την χρήση του Netscaler σε τοπολογία two-arm που θα δούμε παρακάτω.

Η τοπολογία two-arm χαρακτηρίζεται από το γεγονός ότι ένα network interface συνδέεται στο δίκτυο του client και το άλλο στο δίκτυο των servers και με αυτόν τον τρόπο διαχέεται όλη η κίνηση μέσω του Netscaler. Σε αυτήν την συνδεσμολογία ο Netscaler ανήκει σε κάποιο δημόσιο δίκτυο και οι servers είτε σε ιδιωτικό δίκτυο (Traditional) είτε σε δημόσιο (Transparent), ενώ δίνεται η δυνατότητα στον διαχειριστή να τοποθετήσει τους servers (web-servers συγκεκριμένα, όπως φαίνεται στην παρακάτω εικόνα) πίσω από τον Netscaler.



Εικόνα 3-2. Τοπολογία Two-Arm

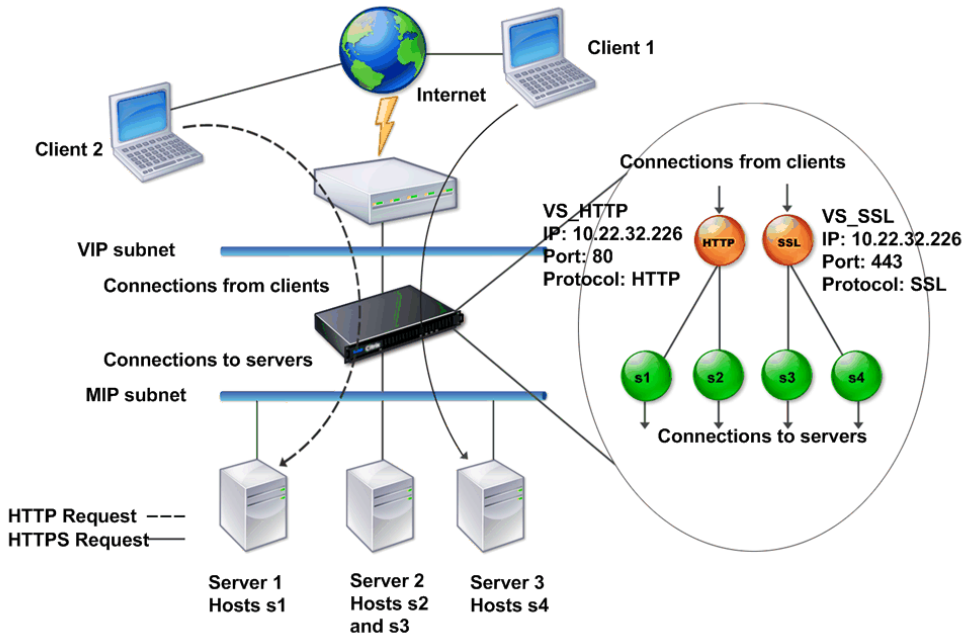
Σε περιπτώσεις όπως οι συναλλαγές με πιστωτικές κάρτες, όπου οι IPs των client-hosts θα πρέπει να ταιριάζουν με τις εγγραφές DNS θα πρέπει να ενεργοποιηθεί η λειτουργία RNAT στον Netscaler για την μετάφραση των δημόσιων IPs στις ανάλογες ιδιωτικές που αντιστοιχούν στους application-servers.

Επιπροσθέτως σε περιπτώσεις πολλαπλών υποδικτύων DMZs μπορεί να χρησιμοποιηθεί ένας Netscaler όπως για παράδειγμα ο hardware-based SDX που μπορεί να περιέχει πολλά instances. Μέσω της διαδικασίας VLAN tagging να δρομολογηθεί η κίνηση από το firewall στον Netscaler και από κει στα switches και με την λειτουργία MAC based forwarding του Netscaler κάθε VLAN να αντιστοιχηθεί σε έναν εικονικό Netscaler. Αυτός ο τρόπος είναι κατάλληλος για παρόχους υπηρεσιών cloud καθώς με μία μόνο συσκευή Netscaler μπορούν να φιλοξενήσουν πολλά διαφορετικά ιδιωτικά δίκτυα πελατών τους.

3.2.3 *Επικοινωνία με Clients και Servers*

Ο Netscaler βρίσκεται μπροστά από ένα σύμπλεγμα διακομιστών (server-farm), λειτουργώντας ως ένας αόρατος TCP proxy μεταξύ clients και servers χωρίς να απαιτείται οποιαδήποτε διαμόρφωση από την πλευρά των clients-servers. Αυτή η λειτουργία ονομάζεται *Request Switching technology* και είναι μία από τις βασικές του Netscaler, μέσω της οποίας δίνεται η δυνατότητα διατήρησης των μόνιμων συνδέσεων και διαχείρισης της κίνησης στο επίπεδο εφαρμογής. Αυτό οφείλεται στην δυνατότητα του Netscaler να διαχωρίζει ένα αίτημα HTTP από την σύνδεση TCP στην οποία παραδίδεται το αίτημα. Πιο συγκεκριμένα στην περίπτωση που ο client επιθυμεί μία ασφαλή σύνδεση σε μία εφαρμογή ο Netscaler εκτελεί την απαραίτητη SSL διαδικασία πριν σταλεί η κίνηση στον server.

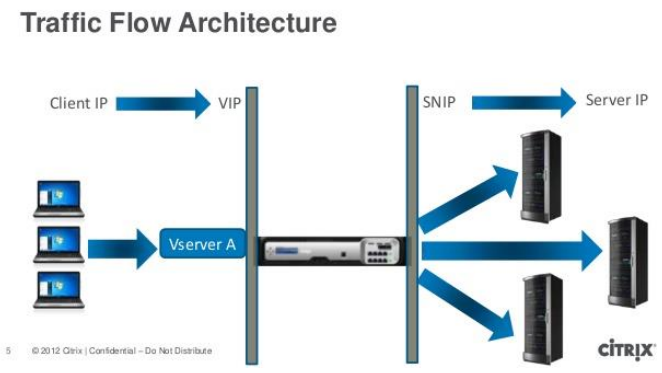
Για να πραγματοποιηθεί αποτελεσματικά και με ασφάλεια η σύνδεση του client προς τους servers που φιλοξενούν τις εφαρμογές, ο Netscaler χρησιμοποιεί ένα σύνολο διευθύνσεων IP τις οποίες και αντιστοιχεί σε εικονικές οντότητες “virtual servers” οι οποίες αποτελούν τα δομικά στοιχεία για την διαχείριση της κυκλοφορίας και εξυπηρετούν διαφορετικές ροές κίνησης. Οι virtual-servers εκπροσωπούν διευθύνσεις IP, πόρτες και πρωτόκολλα επεξεργασίας της κυκλοφορίας καθώς οι clients αποκτούν πρόσβαση σε εφαρμογές-services μέσω αυτών. Ο κάθε vserver αντιπροσωπεύει κάποια ομάδα από servers και οι υπηρεσίες “services” αντιπροσωπεύουν τις εφαρμογές που είναι εγκατεστημένες στον κάθε server.



Εικόνα 3-3. Ροή κυκλοφορίας μέσω Vservers

Οι vservers μπορούν να κατηγοριοποιηθούν στις ακόλουθες κατηγορίες:
Load balancing virtual servers, λαμβάνει και κατευθύνει την κίνηση στον κατάλληλο server βάση της μεθόδου εξισορρόπησης φορτίου.
Cache redirection virtual server, κατευθύνει τα αιτήματα των clients με δυναμικό περιεχόμενο στους κατάλληλους servers και τα αιτήματα στατικού περιεχομένου σε servers με κρυφή μνήμη “cache servers” για γρηγορότερα αποτελέσματα, αυτή η κατηγορία μπορεί να συνεργαστεί αποτελεσματικά με την πρώτη κατηγορία που αναφέραμε.
Content switching virtual server, οδηγεί την κίνηση σε έναν server με βάση το περιεχόμενο της αίτησης του client.
Virtual private network (VPN) virtual server, αποκρυπτογραφεί την κίνηση και την αποστέλλει στους servers του ιδιωτικού δικτύου που εξυπηρετούν την κατάλληλη εφαρμογή.
SSL virtual server, αποκρυπτογραφεί την κίνηση SSL και κατευθύνει το αίτημα στον κατάλληλο server.

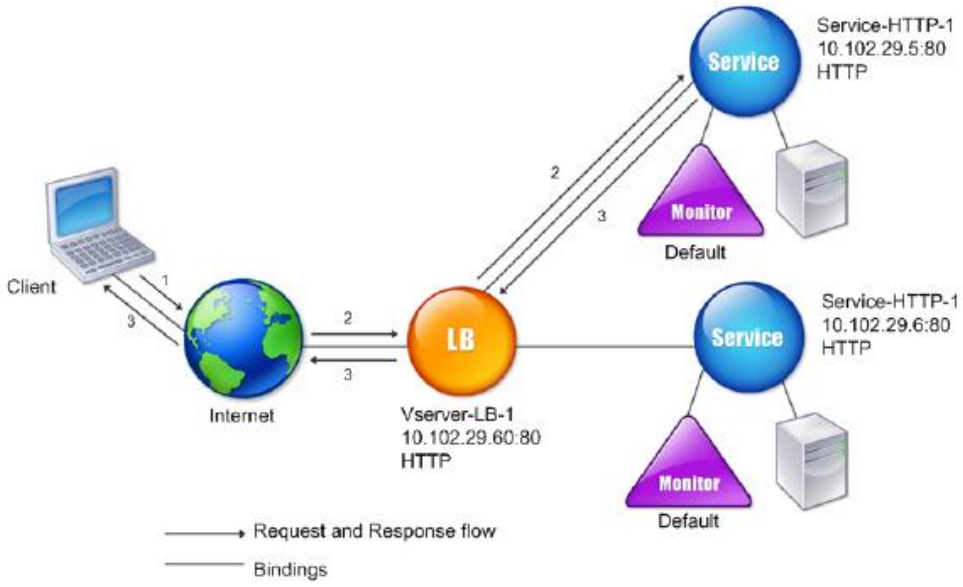
Οι IPs που χρησιμοποιεί ο Netscaler είναι οι εξής:
NetScaler IP address (NSIP), μέσω της οποίας αποκτά κάποιος πρόσβαση στον Netscaler για λόγους διαχείρισης και παραμετροποίησης.
Subnet IP address (SNIP), στις περιπτώσεις που ο Nescaler είναι συνδεδεμένος με πολλαπλά υποδίκτυα η διεύθυνση αυτή υποδηλώνει το υποδίκτυο με το οποίο πρέπει να επικοινωνήσει.
Mapped IP address (MIP), χρησιμοποιείται για την σύνδεση με τους servers. Όταν παραλαμβάνει ένα πακέτο αντικαθιστά την διεύθυνση source IP με την MIP για να αποσταλεί στον κατάλληλο server. Συνήθως χρησιμοποιείται σε περίπτωση που δεν υπάρχει η διεύθυνση SNIP.
Virtual server IP address (VIP), η δημόσια IP στην οποία συνδέονται και γίνεται η ταυτοποίηση των clients.



Εικόνα 3-4. Netscaler IPs

Ο Netscaler μεταφράζει την IP διεύθυνση πριν παραδώσει το πακέτο σε έναν server καθώς ο client συνδέεται σε μία VIP του Netscaler και όχι απευθείας στον ίδιο τον server. Ο Netscaler με τη σειρά του χρησιμοποιεί μία SNIP και αν δεν υπάρχει αυτή μια MIP έτσι ώστε να κατευθύνει την κίνηση στον κατάλληλο server.

Στην παρακάτω εικόνα ο Netscaler έχει ρυθμιστεί για να λειτουργεί ως εξισορροπητής φορτίου, διανέμει τα αιτήματα των clients σε διάφορους servers έτσι ώστε να βελτιστοποιεί την αξιοποίηση των πόρων. Τα βασικά στοιχεία ώστε να ανταπεξέλθουν στο ρόλο της εξισορρόπησης φορτίου είναι η ρύθμιση των εικονικών οντοτήτων και οι υπηρεσίες “services”. Θα πρέπει να δημιουργηθούν services για κάθε server και να δεσμευτούν σε κάποιον vserver καθώς όταν ο client στέλνει ένα αίτημα στον Netscaler αυτός χρησιμοποιεί μια εικονική οντότητα και αποφασίζει μέσω του αλγορίθμου εξισορρόπησης φορτίου ποιος server είναι διαθέσιμος και θα εξυπηρετήσει το αίτημα.



Εικόνα 3-5. Η διαδικασία εξισορρόπησης φορτίου

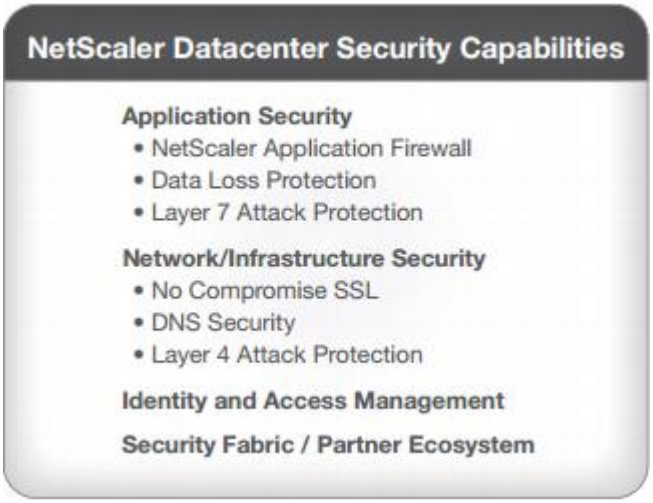
Ο αλγόριθμος εξισορρόπησης φορτίου μπορεί να ρυθμιστεί από τον διαχειριστή ο οποίος κρίνει ποιες παραμέτρους θα χρησιμοποιήσει για την βελτιστοποίηση του.

3.3 Χαρακτηριστικά Ασφαλείας

Η ανάγκη για ισχυρή ασφάλεια στις υποδομές πληροφορικής δεν ήταν ποτέ μεγαλύτερη από ότι είναι στις μέρες μας όπου η αύξηση των κινδύνων είναι γεγονός αλλά και οι ευαίσθητες πληροφορίες που διακινούνται μέσω των πληροφοριακών

συστημάτων ολοένα και αυξάνονται. Αν αναλογιστούμε και τις οικονομικές πιέσεις των καιρών που οδηγούν στην απαίτηση της αύξησης της ασφάλειας αλλά με μικρότερη οικονομική επιβάρυνση, αντιλαμβανόμαστε ότι η ασφάλεια θα πρέπει να βασιστεί στην ήδη υπάρχουσα υποδομή.

Ο Citrix Netscaler ADC είναι το στρατηγικό συστατικό που δίνει μια κατάλληλη λύση για την κατασκευή δικτύων επιχειρήσεων προσφέροντας εκτεταμένες δυνατότητες ασφαλείας ενώ παράλληλα ελαχιστοποιεί τις επενδύσεις μεγάλου κόστους που απαιτούν οι αυτόνομες λύσεις ασφαλείας. Παρακάτω θα δούμε αναλυτικότερα την ασφάλεια που προσφέρει σε επίπεδο εφαρμογής, δικτύου – υποδομής καθώς και στην διαχείριση της ταυτοποίησης και πρόσβασης των χρηστών.



3.3.1 Ασφάλεια σε επίπεδο εφαρμογής - Application Firewall

Τα παραδοσιακά Firewalls δεν έχουν την δυνατότητα ελέγχου που απαιτείται για την αντιμετώπιση μεγάλου ποσοστού επιθέσεων που έχουν ως στόχο το επίπεδο εφαρμογής. Σε αυτό το σημείο ο Netscaler υπερέχει εμποδίζοντας γνωστές και άγνωστες επιθέσεις ενάντια σε web-services, χρησιμοποιώντας ένα υβριδικό μοντέλο ασφαλείας και αναλύοντας την κίνηση προς όλες τις κατευθύνσεις, συμπεριλαμβανομένων και των κρυπτογραφημένων μέσω SSL επικοινωνιών, εξουδετερώνει ένα μεγάλο φάσμα απειλών χωρίς να απαιτείται κάποια τροποποίηση στις εφαρμογές.

Το *υβριδικό μοντέλο* είναι ένας συνδυασμός δύο μηχανισμών, positive engine που αντιλαμβάνεται μέσω πολιτικών την επιτρεπτή αλληλεπίδραση χρήστη-εφαρμογής εμποδίζοντας την κίνηση η οποία ξεφεύγει από τα όρια της αλληλεπίδρασης που έχουν τεθεί. Negative engine που χρησιμοποιεί υπογραφές για να αποτρέψει γνωστές επιθέσεις κατά των εφαρμογών.

Για την αποφυγή *επιθέσεων XML* ενσωματώνει ένα πλούσιο σύνολο μέτρων προστασίας συμπεριλαμβανομένων, της επικύρωσης της δομής-schema για τον

έλεγχο των μηνυμάτων SOAP και των ωφέλιμων XML φορτίων, την ικανότητα παρεμπόδισης συνημμένων σε XML που περιέχουν κακόβουλα εκτελέσιμα αρχεία και αποφυγής τεχνικών XPath injections για απόκτηση μη εξουσιοδοτημένης πρόσβασης.

Προστασία έναντι *δυναμικών στοιχείων* όπως cookies, form fields, session-specific URLs, που χρησιμοποιούνται κατά την αλληλεπίδραση χρήστη-εφαρμογής και σε πολλές περιπτώσεις ο επιτιθέμενος έχει ως σκοπό να εκμεταλλευτεί αυτήν την σχέση εμπιστοσύνης. Αυτή η περίπτωση αντιμετωπίζεται από τον μηχανισμό positive engine η οποία και καθορίζει την αναμενόμενη συμπεριφορά των web-applications και παράγει προσαρμοσμένες πολιτικές αναγνωρίσιμες από τον διαχειριστή ο οποίος μπορεί να τις αναπτύξει και για την προστασία άλλων εφαρμογών.

Η υπηρεσία *IP reputation* ενισχύει τον Netscaler ενημερώνοντας τον με μία λίστα στην οποία εμπεριέχονται IPs συσκευών από τις οποίες προέρχονται κακόβουλες ενέργειες. Η υπηρεσία αυτή ενσωματώνει την συνεχή τροφοδοσία και ανανέωση της IP λίστας σε διαστήματα λίγων λεπτών, ουσιαστικά λειτουργεί σε πραγματικό χρόνο με αποτέλεσμα να μην δημιουργούνται ποτέ out-of-date λίστες.

Μέσω της διαδικασίας *φιλτραρίσματος περιεχομένου* δίδεται η δυνατότητα να εξεταστεί το τμήμα της κεφαλίδας “header” της αίτησης ή απάντησης HTTP μέσω “regular expressions”, έτσι στην περίπτωση ενός πολύπλοκου web-site με εκτεταμένη χρήση scripts και πρόσβασης σε δεδομένα βάσεων, η υπηρεσία αυτή του application firewall μπορεί να προστατέψει από επιθετικές ενέργειες.

Η απροσδόκητη διαρροή ευαίσθητων δεδομένων από έναν application-server που μπορεί να προέλθει από μία επιτυχημένη επίθεση στην εφαρμογή, από κακό σχεδιασμό της εφαρμογής ή από κακή χρήση ενός εξουσιοδοτημένου χρήστη μπορούν να αντιμετωπιστούν από τον διαχειριστή του δικτύου μέσω του χαρακτηριστικού “Safe Object data checks” του Netscaler. Δίδεται η δυνατότητα στον διαχειριστή να δημιουργήσει κανόνες μέσω των οποίων το firewall μπορεί να προστατέψει την υποδομή από διαρροές τέτοιων δεδομένων με τους παρακάτω τρόπους:

- Εμποδίζοντας την απάντηση στο αίτημα του χρήστη
- Προστατεύοντας περαιτέρω την ευαίσθητη πληροφορία
- Αφαιρώντας την ευαίσθητη πληροφορία από την απάντηση που στέλνεται στον χρήστη

Κατά την χρήση αριθμών πιστωτικών καρτών μέσω κάποιας εφαρμογής ελέγχονται οι πληροφορίες και τα δεδομένα ωφέλιμου φορτίου έτσι ώστε να αποφευχθούν τυχόν false-negatives ενώ συντελείται ταύτιση συμβολοσειρών μέσω αλγόριθμου για την

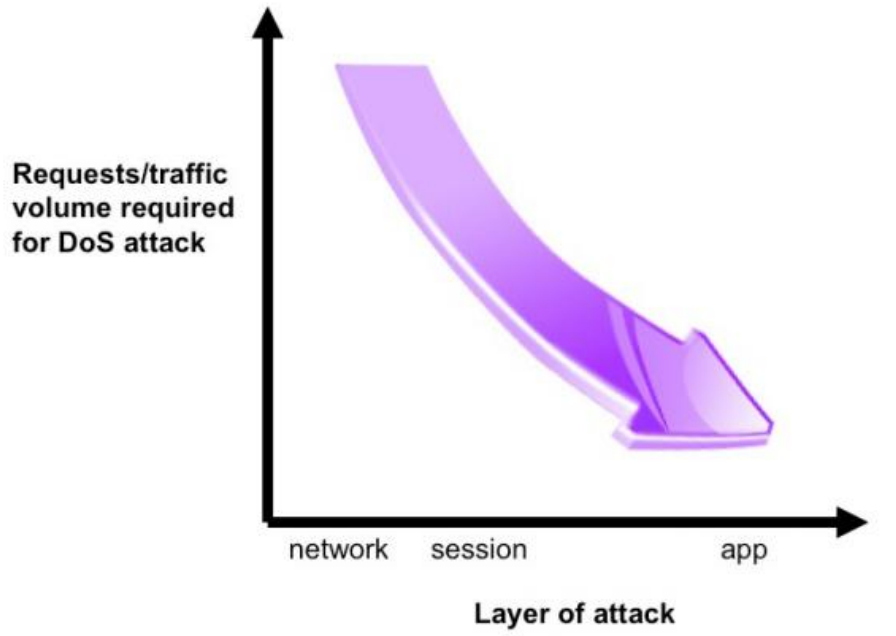
αποφυγή false-positives. Σε περίπτωση που η αποστολή αριθμών πιστωτικών καρτών δεν είναι αναγκαία μπορεί ο διαχειριστής μέσω κανόνων που θα δημιουργήσει να απαγορεύσει την αποστολή τέτοιων στοιχείων ή να την επιτρέψει μέσω περιορισμών (π.χ. εμφάνιση μόνο των τελευταίων ψηφίων).

Επιπρόσθετοι μηχανισμοί που χρησιμοποιεί ο Netscaler για την παροχή προστασίας σε επίπεδο εφαρμογής “Layer7 of OSI Model” είναι οι εξής:

HTTP protocol validations, επιβάλλοντας διεθνώς αναγνωρισμένα “security standards” και βέλτιστες πρακτικές για την χρήση του πρωτοκόλλου HTTP, αποτρέπει την κακόβουλη συμπεριφορά αιτημάτων που χρησιμοποιούν το πρωτόκολλο αυτό. Επιπρόσθετοι έλεγχοι μπορούν να υπάρξουν αξιοποιώντας την διαδικασία φιλτραρίσματος περιεχομένου, τις αμφίδρομες δυνατότητες του μηχανισμού “HTTP rewrite module” για την πρόληψη της πρόσβασης των χρηστών σε συγκεκριμένα μέρη κάποιου web-site, την υπεράσπιση ενάντια σε “HTTP-based” απειλές και την απομάκρυνση πληροφοριών από τις απαντήσεις που στέλνονται στους χρήστες, και οι οποίες μπορούν να χρησιμοποιηθούν για να εκτελεστεί μια επίθεση.

HTTP DoS protection, μία καινοτόμος μέθοδος που χρησιμοποιείται για την αποφυγή επιθέσεων DDoS είναι όταν ανιχνεύεται μία τέτοια κατάσταση, το οποίο επιτυγχάνεται μέσω ρυθμιζόμενου ορίου για τα αιτήματα που βρίσκονται στην ουρά, στέλνεται σε ένα συγκεκριμένο ποσοστό χρηστών μία πρόκληση “challenge” χαμηλού υπολογιστικού αντίκτυπου, στην οποία οι νόμιμοι χρήστες μπορούν να ανταποκριθούν σωστά ενώ η πηγή από την οποία προέρχεται η επίθεση δεν μπορεί να ανταποκριθεί. Επίσης άλλοι μηχανισμοί όπως προσαρμοσμένα χρονικά όρια μπορούν να χρησιμοποιηθούν για την αποφυγή απειλών DDoS όπως SlowRead και SlowPost.

Στην παρακάτω εικόνα φαίνεται η ασυμμετρία που παρουσιάζει μια επίθεση DDoS, στοιχείο το οποίο δυσκολεύει τον εντοπισμό της επίθεσης καθώς σε επίπεδο εφαρμογής η κίνηση που παρουσιάζει μειώνεται.



Εικόνα 3-6. Ασυμμετρία επίθεσης DDoS

Μια επιπλέον προσέγγιση για την απόκρουση της τεχνικής DDoS είναι να αποτραπεί η υπερφόρτωση του δικτύου και των servers ανακατευθύνοντας την κίνηση όταν υπερβεί ένα συγκεκριμένο όριο. Για αυτό το σκοπό ο μηχανισμός *AppExpert* ελέγχει τον ρυθμό ενεργοποιώντας πολιτικές του Netscaler που βασίζονται στην σύνδεση, τα αιτήματα, ή τον ρυθμό δεδομένων από ή προς ένα συγκεκριμένο υπολογιστικό πόρο (π.χ. vserver, domain, URL). Άλλες σχετικές δυνατότητες που παρέχονται είναι:
Surge protection, για την απόσβεση των επιπτώσεων στις ώρες αιχμής της κυκλοφορίας στους servers,
Priority queuing, για να εξασφαλιστεί η εξυπηρέτηση των κρίσιμων πόρων από τους μη κρίσιμους κατά την διάρκεια περιόδων υψηλής ζήτησης.

Increasing difficulty of detection

	Sample Attacks	NetScaler Mitigation Features
Application	GET and malicious POST floods; slowloris, slow POST, and other low-bandwidth variants	Application protocol validation, surge protection, priority queuing, HTTP flood protection, HTTP low-bandwidth attack protection
Connection and Session	Connection floods, SSL floods, DNS floods (udp, query, nxdomain)	Full-proxy architecture, high- performance design, intelligent memory handling, extensive DNS protection
Network	Syn, UDP, ICMP, PUSH and ACK floods; LAND, smurf, and teardrop attacks	Embedded defenses, default deny security model, protocol validation, rate limiting

Πίνακας 3-2. Χαρακτηριστικά μετρίασης επιθέσεων DDoS

3.3.2 Ασφάλεια σε επίπεδο δικτύου και υποδομής

Ο Netscaler ενσωματώνει επίσης δυνατότητες ασφαλείας σε επίπεδο δικτύου και υποδομής. Οι πιο αξιοσημείωτες είναι η υποστήριξη κρυπτογράφησης SSL, ασφάλεια DNS και προστασία επιπέδου “Layer 4”.

Στην *κρυπτογράφηση SSL* προκύπτουν δύο σημαντικά ζητήματα που αφορούν την επιβάρυνση των υπολογιστικών πόρων της υποδομής. Αρχικά η ανάγκη για κρυπτογράφηση στο σύνολο της εφαρμογής όχι μόνο ενός ευαίσθητου σημείου της επιφέρει υπερφόρτωση της υποδομής. Το δεύτερο ζήτημα έχει να κάνει με την χρήση κλειδιών κρυπτογράφησης 2048-bit αλλά και μεγαλύτερων με αποτέλεσμα την αύξηση των απαιτήσεων επεξεργασίας. Η μετάβαση αυτή προήλθε μετά από οδηγίες που εκδόθηκαν από το εθνικό ινστιτούτο των ΗΠΑ (NIST) το 2013 καθώς κορυφαίοι προμηθευτές προγραμμάτων περιήγησης οδηγήθηκαν στην απόφαση να μην υποστηρίζουν web-sites που χρησιμοποιούν πιστοποιητικά με κλειδιά ασθενέστερα των 2048 bits.

Οι συσκευές Netscaler αντιμετώπισαν αυτές τις τάσεις ενσωματώνοντας ειδικό υλικό “SSL acceleration hardware” το οποίο μπορεί να υποστηρίξει τη χρήση κλειδιών 2048 και 4096 bits χωρίς να υπάρχει επίπτωση στην απόδοση της υποδομής.

Καθώς η κρυπτογράφηση SSL χρησιμοποιείται όλο και περισσότερο για την προστασία της πνευματικής ιδιοκτησίας, οικονομικών πληροφοριών, προσωπικών δεδομένων των χρηστών και πολλών άλλων εμπιστευτικών πληροφοριών προκύπτει το ζήτημα της ασφάλειας στην διαχείριση των κλειδιών κρυπτογράφησης. Έτσι απαιτείται η προστασία των κλειδιών από ενδεχόμενη επίθεση αλλά και η δημιουργία αντιγράφων ασφαλείας έτσι ώστε να υπάρχει η δυνατότητα ανάκτησης μετά από μία κατάσταση βλάβης ή καταστροφής του συστήματος.

Πέρα από την αύξηση της κίνησης SSL που αποφέρει την επιβάρυνση του συστήματος με την κρυπτογράφηση ή αποκρυπτογράφηση της πληροφορίας η ανάγκη για αύξηση της επεξεργαστικής ισχύς προκύπτει και από τις δραστηριότητες “handshake” και επικύρωσης των πιστοποιητικών, οι οποίες επιβαρύνουν το πρόγραμμα περιήγησης του χρήστη, τον web-server και το bandwidth του δικτύου.

Για να ανταπεξέλθει η εταιρεία Citrix στα παραπάνω ζητήματα, να βελτιστοποιήσει την ασφάλεια της κίνησης και να ανταπεξέλθει στην επιβάρυνση της υποδομής, έχει εγκαθιδρύσει μία συνεργασία με την εταιρεία Thales nShield η οποία διαχειρίζεται ένα μεγάλο σύνολο κλειδιών κρυπτογράφησης SSL σε ένα “FIPS 140-2 Level 3“ πιστοποιημένο περιβάλλον, δίνοντας λύσεις στην ασφαλή διαχείριση των κλειδιών μέσα στο πλαίσιο της υποδομής πληροφορικής.

Μία σύγχρονη υποδομή θα πρέπει να διαθέτει μία ισχυρή ανάπτυξη DNS έτσι ώστε να μην τίθενται σε κίνδυνο η διαθεσιμότητα και προσβασιμότητα των υπηρεσιών. Η λειτουργία DNS proxy mode παρέχει την δυνατότητα εξισορρόπησης φορτίου ενώ και ο Netscaler έχει τη δυνατότητα λειτουργίας ως DNS (ADNS) μεταφράζοντας άμεσα τα αιτήματα IP. Στα παραπάνω σενάρια ο Netscaler παρέχει μια ασφαλή ανάπτυξη με τα ακόλουθα χαρακτηριστικά:

Hardened design, ο DNS δεν βασίζεται σε εφαρμογή ανοιχτού κώδικα “open source BIND” και έτσι δεν είναι ευπαθής στα τρωτά σημεία που έχουν ανακαλυφθεί σε αυτόν.

RFC compliance/enforcement, εκτελείται πλήρη επικύρωση του πρωτοκόλλου και επιβάλλει τον άμεσο αποκλεισμό επιθέσεων που σχετίζονται με λανθασμένες μορφές αιτήσεων DNS.

Native DNS rate limiting, συμβάλει στην αποτροπή επιθέσεων πλημμύρας “DNS flood attacks”, καθώς είναι δυνατό να οριστούν πολιτικές που να θέτουν συγκεκριμένο όριο ή να απορρίπτουν ερωτήματα που εμπίπτουν σε συγκεκριμένες παραμέτρους που έχουν δημιουργηθεί.

Cache poisoning protection with DNSSEC, οι επιθέσεις hi-jacking είναι μια πολύ σημαντική κατηγορία απειλών που περιλαμβάνει έγχυση πλαστών εγγραφών στον DNS. Έτσι ο χρήστης κατευθύνεται από τον ίδιο τον DNS της υποδομής σε κάποιο web-site που ελέγχεται από τον επιτιθέμενο με αποτέλεσμα την υποκλοπή πολύτιμων πληροφοριών. Ο Netscaler προστατεύει την υποδομή ενάντια σε αυτές τις επιθέσεις με δύο τρόπους:

Υποστηρίζει την λειτουργία DNSSEC, μέσω της οποίας ενεργοποιεί την υπογεγραμμένη απάντηση έτσι ώστε οι clients να μπορούν να επικυρώσουν την αυθεντικότητα της απάντησης.

Η τυχαία κατανομή των συναλλαγών του DNS και της πόρτας που χρησιμοποιεί η πηγή δυσκολεύει τον επιτιθέμενο από το να διαφθείρει τις εγγραφές του DNS.

Σε επίπεδο δικτύου “Layer 4” ο Netscaler προστατεύει την υποδομή από επιθέσεις DDoS εξασφαλίζοντας ότι οι back-end servers δεν κατανέμονται μέχρι να θεσπιστεί μια έγκυρη αίτηση ενός client. Έτσι για παράδειγμα για την αποφυγή επιθέσεων “SYN floods”, οι οποίες έχουν ως στόχο την κατανάλωση αρκετών υπολογιστικών πόρων ώστε να καταστεί το σύστημα μη ανταποκρίσιμο, ο Netscaler επιτρέπει την κίνηση αφού ολοκληρωθεί επιτυχώς η ταυτοποίηση του client μέσω της μεθόδου “three-way TCP handshake”

Άλλοι μέθοδοι είναι οι λίστες ελέγχου πρόσβασης ACL σε επίπεδο Layer 3 και Layer 4 που επιτρέπουν την απαραίτητη κίνηση εφαρμογών και αποτρέπουν οτιδήποτε

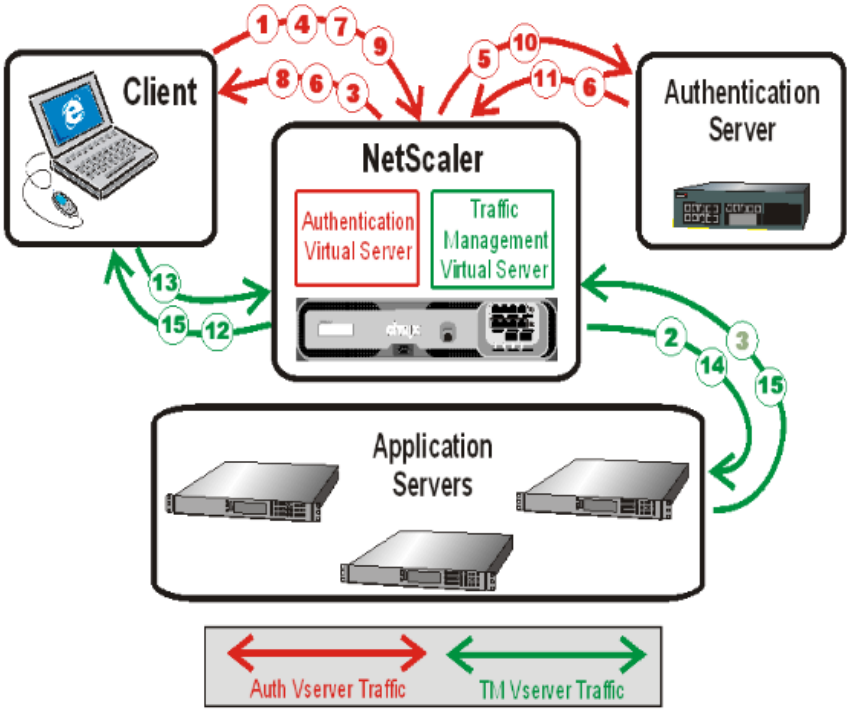
άλλο, οι δυνατότητες surge protection και priority για τις οποίες αναφερθήκαμε προηγουμένως και μία στοίβα " TCP/IP stack" ενισχυμένη για την απόρριψη κίνησης η οποία θα μπορούσε να αποτελεί απειλή για τις συσκευές back-end, την αποτροπή αποκάλυψης σημαντικών πληροφοριών σύνδεσης, όπως IPs ports κλπ, που θα μπορούσαν να είναι χρήσιμες για τον επιτιθέμενο, και την αποφυγή DoS επιθέσεων όπως ICMP flood, pipeline, teardrop, land, fraggle, small/zero window, zombie.

Σε επίπεδο χρήστη ο Netscaler προσφέρει ένα εκτεταμένο σύνολο λειτουργιών AAA,

- *Authentication*, έλεγχος ταυτότητας του χρήστη
- *Authorization*, επαλήθευση και επιβολή των πόρων που είναι εξουσιοδοτημένος να χρησιμοποιήσει ο χρήστης
- *Auditing*, δυνατότητα καταγραφής των δραστηριοτήτων του χρήστη

Τα πλεονεκτήματα της διαδικασίας είναι:

- Βελτίωση της απόδοσης και της ασφάλειας
- Επιπρόσθετη ασφάλεια σε παλαιού τύπου εφαρμογές
- Παροχή συνεπής συμπεριφοράς του χρήστη
- Ενεργοποίηση του μηχανισμού single-sign-on (SSO)
- Απλοποίηση του σχεδιασμού ασφαλείας



Εικόνα 3-7. Η διαδικασία της επικύρωσης μέσω external authentication server

3.3.3 Αξιολόγηση της κατάστασης ασφαλείας

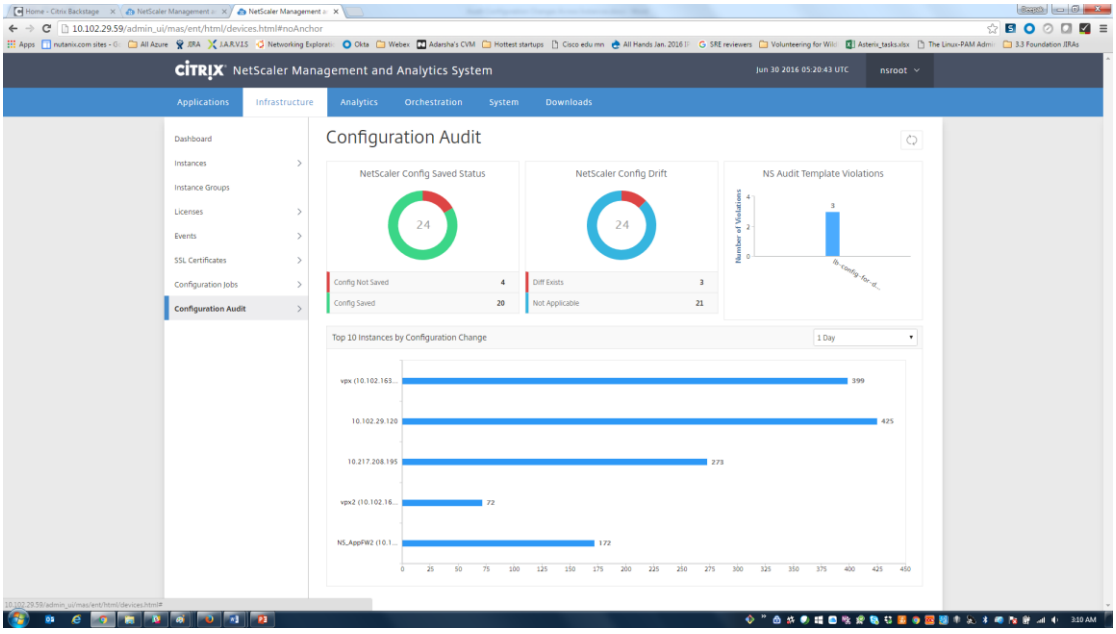
Για την αποτελεσματική προστασία από κακόβουλες επιθέσεις είναι πολύ σημαντικό να παρέχεται διαφάνεια σχετικά με τις απειλές που υπήρξαν στο παρελθόν στο παρόν ή που θα υπάρξουν στο μέλλον, αξιοποιήσιμα δεδομένα σχετικά με επιθέσεις

σε πραγματικό χρόνο και συστάσεις σχετικά με τα αντίμετρα που πρέπει να ληφθούν. Ο Netscaler παρέχει αυτές τις πληροφορίες “security insight” που βοηθούν στην αξιολόγηση της κατάστασης ασφαλείας των εφαρμογών και στη λήψη επιπρόσθετων μέτρων που ίσως απαιτούνται.
Αυτή η λύση περιλαμβάνεται στο “NetScaler Insight Center” και παράγει περιοδικά αναφορές που βασίζονται στις ρυθμίσεις ασφαλείας του συστήματος. Οι αναφορές αυτές περιλαμβάνουν τις παρακάτω πληροφορίες:

Threat Index, ένα σύστημα που υποδεικνύει την κρισιμότητα της απειλής σχετικά με το αν η εφαρμογή προστατεύεται από μία συσκευή Netscaler, η κρισιμότητα υποδεικνύεται με βάση μία τιμή που κυμαίνεται από το 1 (low) έως το 7 (high). Ο δείκτης απειλής βασίζεται σε πληροφορίες όπως το είδος της παραβίασης, την τοποθεσία, τις πληροφορίες για τον client.

Safety Index, αυτός ο δείκτης δείχνει σε τι βαθμό έχει ρυθμιστεί ο Netscaler για να προστατεύσει την υποδομή από παραβιάσεις και χρησιμοποιεί και αυτός μία τιμή που κυμαίνεται από το 1 (low) έως το 7 (high) για να γίνει κατανοητός ο βαθμός του κινδύνου ασφαλείας. Ο δείκτης ασφαλείας λαμβάνει υπόψιν όλες τις παραμέτρους, για παράδειγμα αν υπάρχει αυστηρή διαμόρφωση στο application firewall αλλά επίσης έχει υιοθετηθεί ένας αδύναμος κωδικός, αποδίδεται ένας χαμηλός δείκτης ασφαλείας.

Actionable Information, οι πληροφορίες που χρειάζεται ο διαχειριστής για να προβεί στην μείωση του δείκτη απειλής και στην αύξηση του δείκτη ασφάλειας που βελτιώνει σημαντικά την ασφάλεια των εφαρμογών. Για παράδειγμα είναι διαθέσιμες πληροφορίες για παραβιάσεις, ελλιπής ρυθμίσεις του application firewall και άλλων χαρακτηριστικών ασφαλείας.



Εικόνα 3-8. NetScaler Insight Center

4 Ανάπτυξη του συστήματος και εφαρμογή κανόνων ασφαλείας

Στο τέταρτο κεφάλαιο δίνονται οι τεχνικές λεπτομέρειες του περιβάλλοντος που αναπτύχθηκε για τις ανάγκες της διπλωματικής εργασίας και την υλοποίηση σε τεχνικό επίπεδο όλων όσων αναφέρθηκαν στα παραπάνω κεφάλαια.

Η υλοποίηση της υποδομής στηρίζεται στη δημιουργία εικονικών μηχανημάτων (Virtual Machines) σε περιβάλλον Azure Cloud πάνω στο οποίο αναπτύχθηκε η πλατφόρμα Citrix XenDesktop και XenApp (ver. 7.11), αλλά και ένα εικονικό μηχάνημα που φιλοξενεί έναν Internet Information Server (IIS ver.8) με public IP.

Τέλος για την πραγματοποίηση των επιθέσεων αλλά και την δημιουργία Apache Web Server χρησιμοποιήθηκε η τεχνολογία VMware Workstation (ver. 12.5) στην οποία αναπτύχθηκαν δύο εικονικά μηχανήματα βασισμένα σε λειτουργικό σύστημα Linux.

4.1 Σχεδιασμός Συστήματος – Αρχιτεκτονική

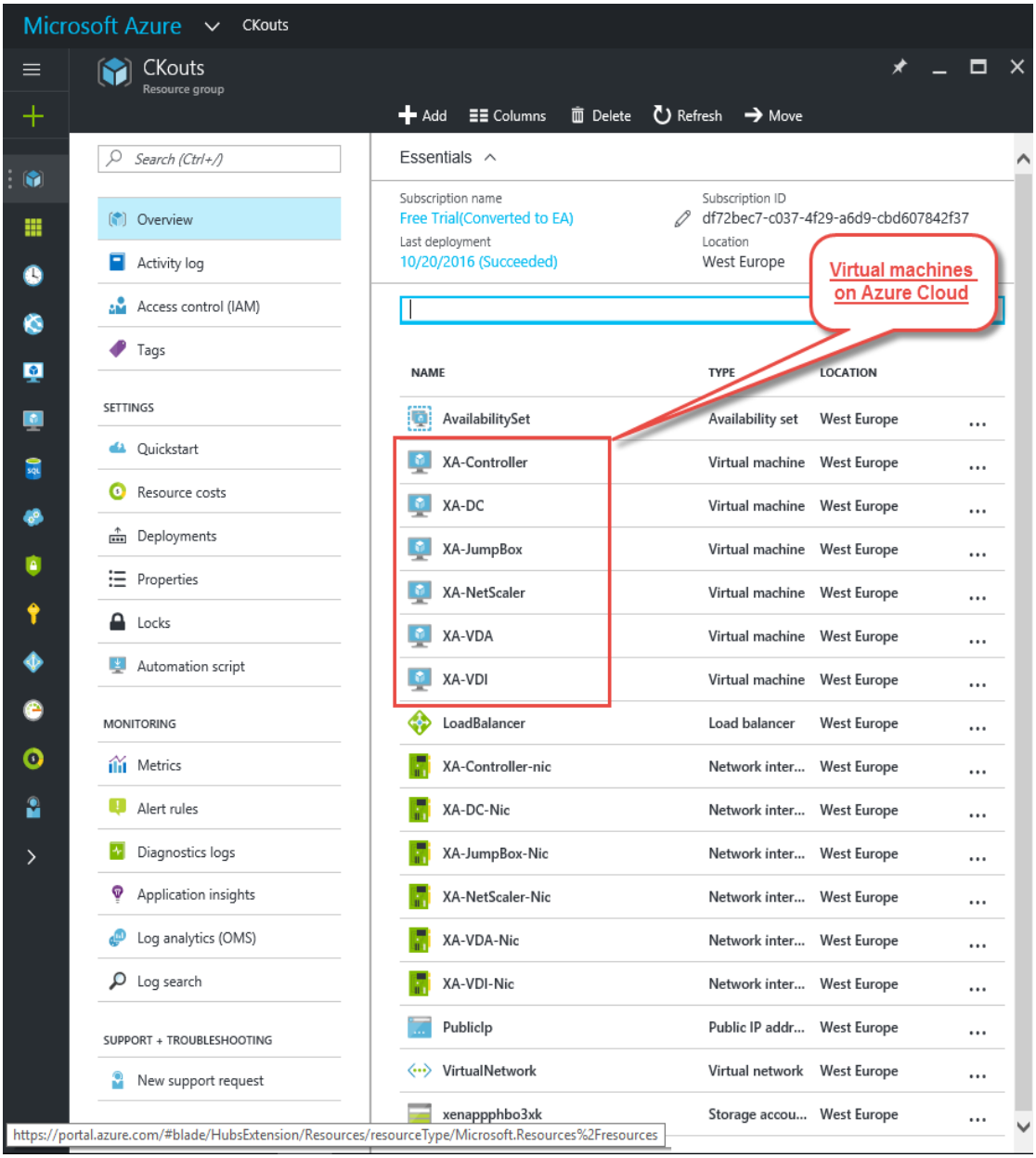
Στις παρακάτω ενότητες δίνονται λεπτομέρειες σχετικά με το είδος των συστημάτων που αναπτύχθηκαν, την τοπολογία όπου αυτά βρίσκονται και την λειτουργία αυτών με σκοπό την κατανόηση της υποδομής που έχει δημιουργηθεί.

4.1.1 Μέρη από τα οποία αποτελείται το σύστημα

Citrix on Azure Cloud

Component	Machine Name	Description
Domain Controller	XA-DC	A Windows Server 2012 R2 Active Directory Domain Controller
Citrix NetScaler	XA-NetScaler	NetScaler 11.x VPX Gateway which allows users to access apps and desktops from the deployment
Citrix XenApp Controller	XA-Controller	Includes XenApp Delivery Controller,SQL Server Express, Citrix License Server, StoreFront 3.5, and Director
Citrix Virtual Desktop Agents	XA-VDA	Windows Server 2012 R2 with the XenApp VDA installed in hosted-shared (multi-session) mode.
	XA-VDI	Windows Server 2012 R2 with the XenApp VDA installed in Server VDI mode.
Jump Box	XA-JumpBox	Windows Server 2012 R2 configured to allow RDP access for administration

Πίνακας 4-1. Μέρη Συστήματος

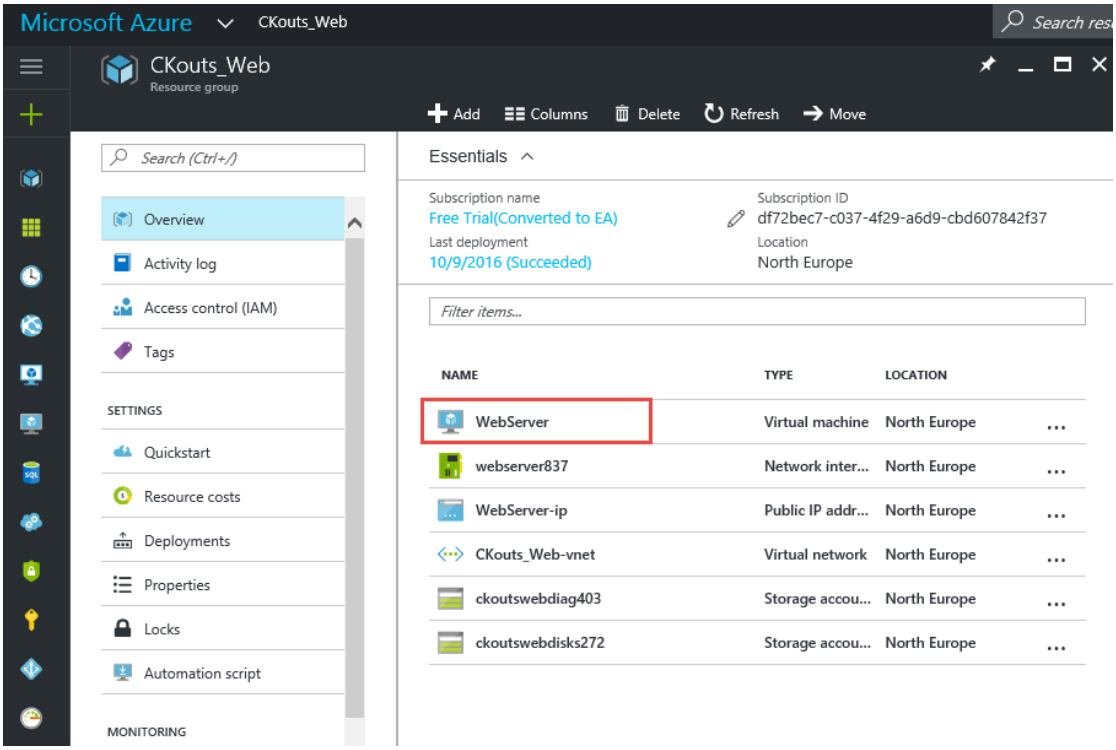


Εικόνα 4-1. Azure Console

Internet Information Server on Azure Cloud

Component	Machine Name	Description
IIS Server	WebServer	IIS ver.8 on Windows Server 2012 R2

Πίνακας 4-2. IIS Server

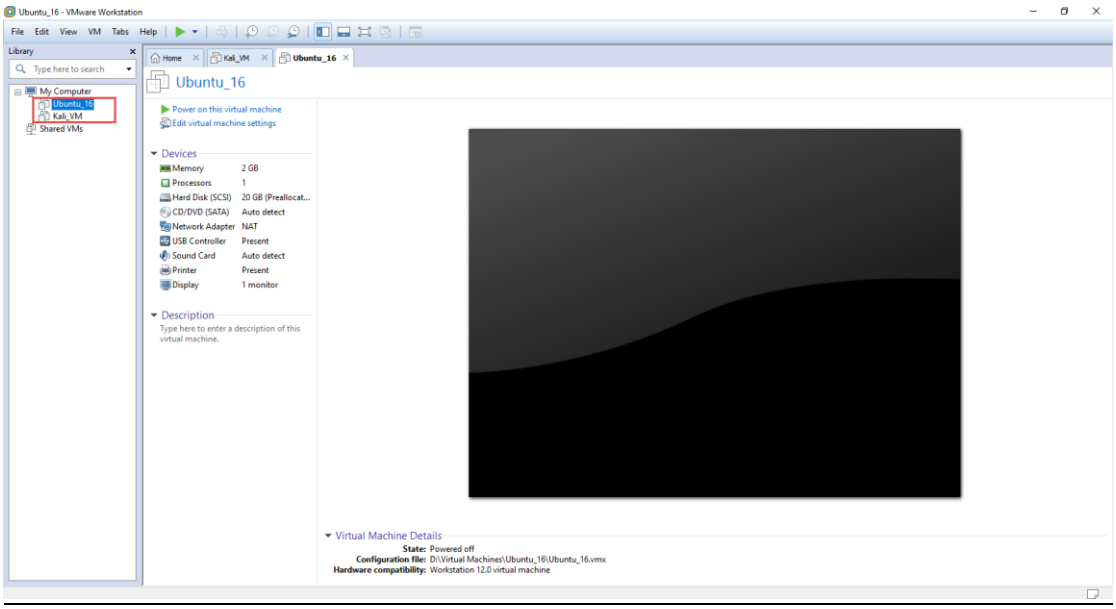


Εικόνα 4-2. Azure Console IIS

VMware Workstation on Local Client

Component	Machine Name	Description
Linux Ubuntu	Ubuntu_16	Ubuntu-16.04.1 with Apache 2 web server
Linux Kali	Kali_VM	Kali-linux-2016.2

Πίνακας 4-3. Linux Machines

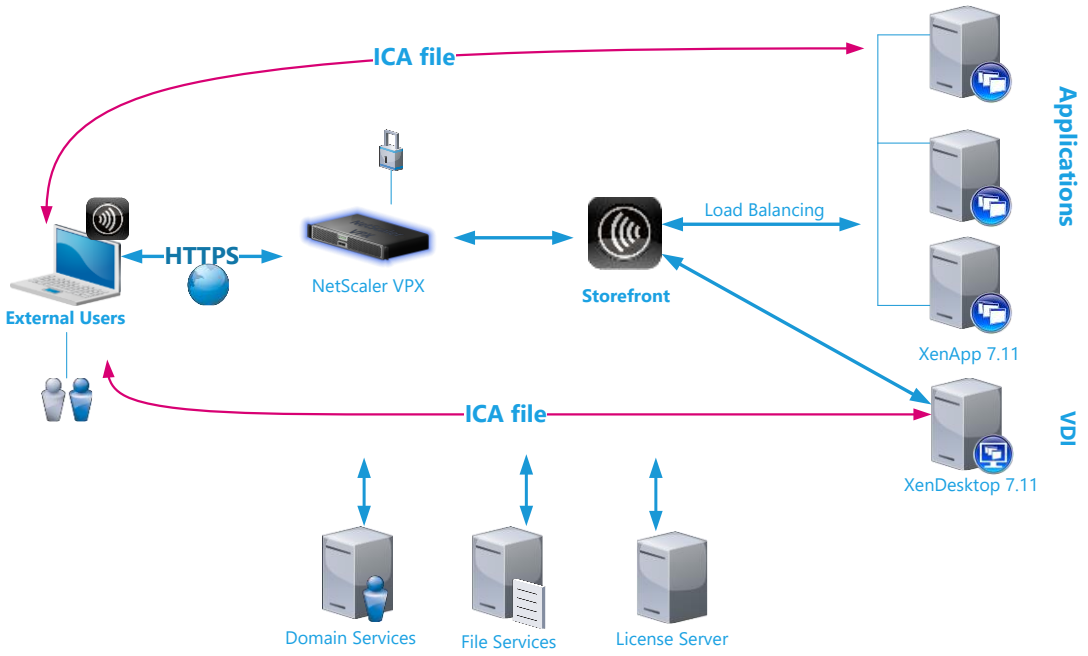


Εικόνα 4-3. VMware WorkStation

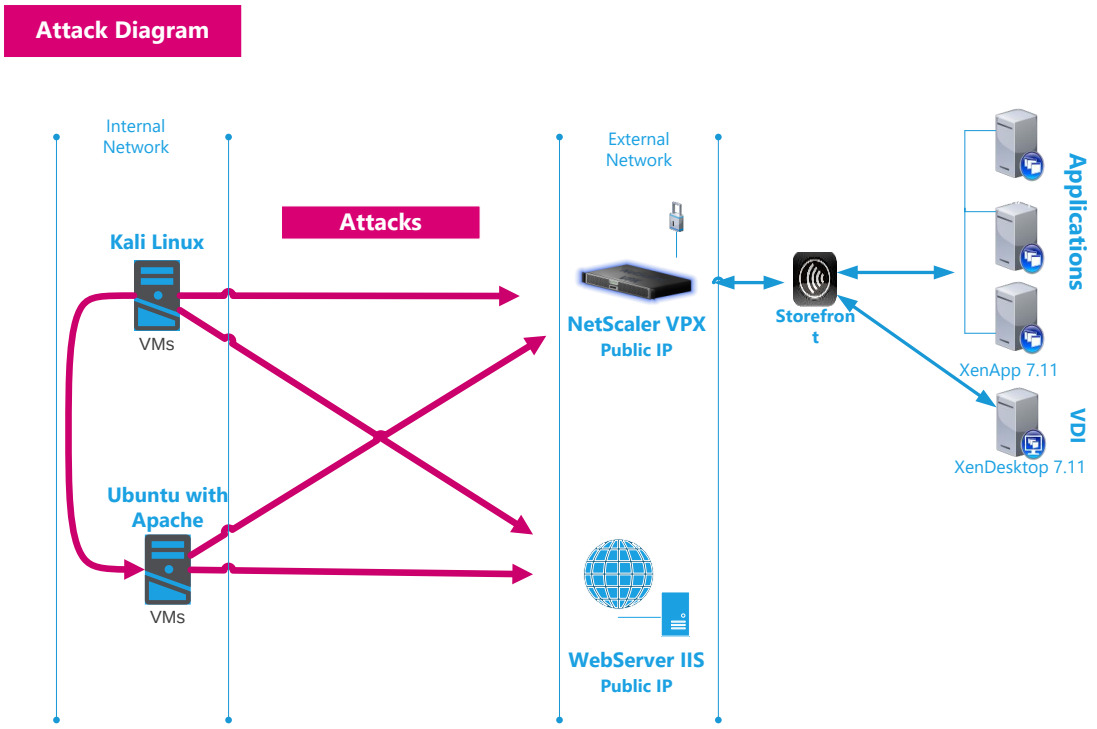
4.1.2 Τοπολογία

Στο πρώτο σχήμα διακρίνουμε την τοπολογία του περιβάλλοντος Citrix ενώ στο δεύτερο τη συνολική τοπολογία όπου εκτελούνται και τα διάφορα είδη επιθέσεων που θα εξετάσουμε παρακάτω.

Citrix XenApp 7.11



Εικόνα 4-4. Citrix Topology

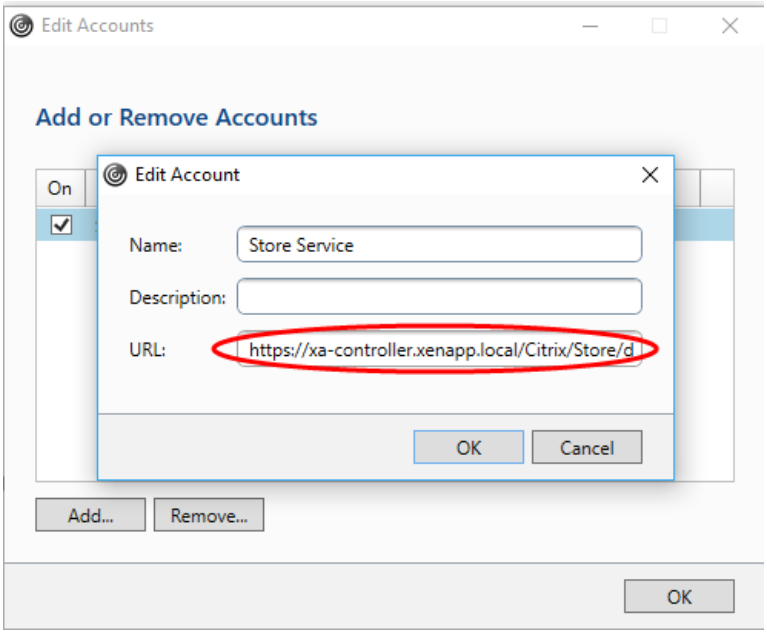


Εικόνα 4-5. Attack Topology

4.1.3 Λειτουργία του συστήματος από την πλευρά του χρήστη

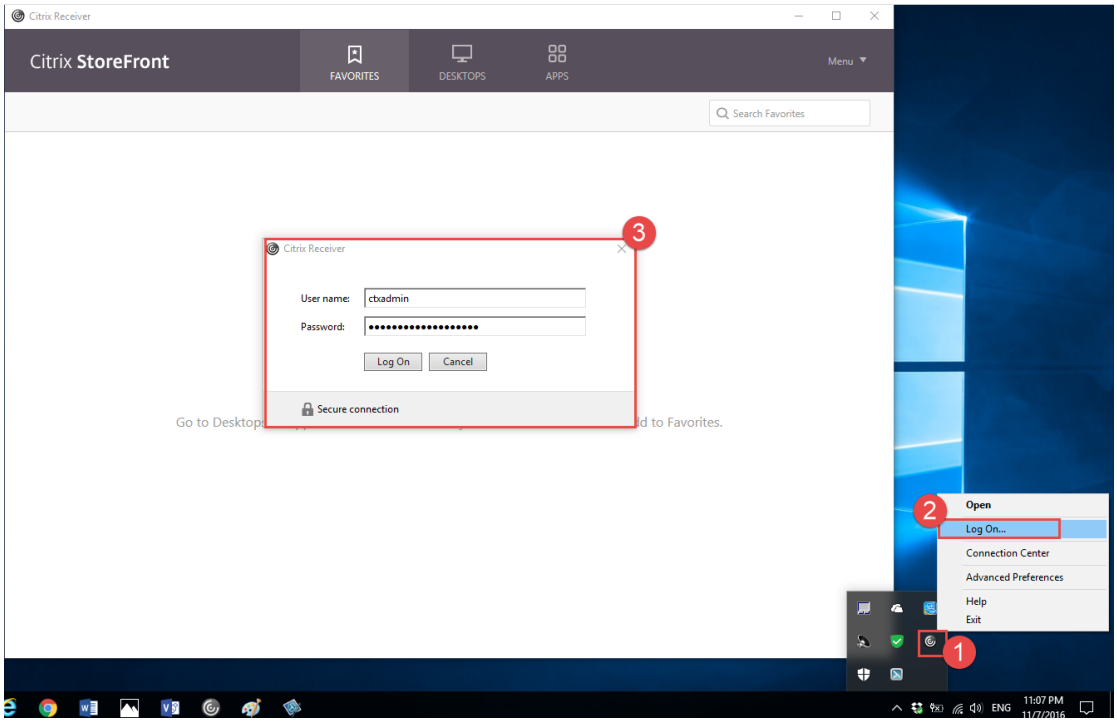
Η χρήση της υποδομής Citrix από την πλευρά του χρήστη γίνεται μέσω της παρακάτω απλής διαδικασίας:

- ✓ Ο χρήστης ανοίγει τον Citrix receiver ο οποίος έχει ρυθμιστεί κατάλληλα με το URL στο οποίο θα εκτελεστεί η επικοινωνία



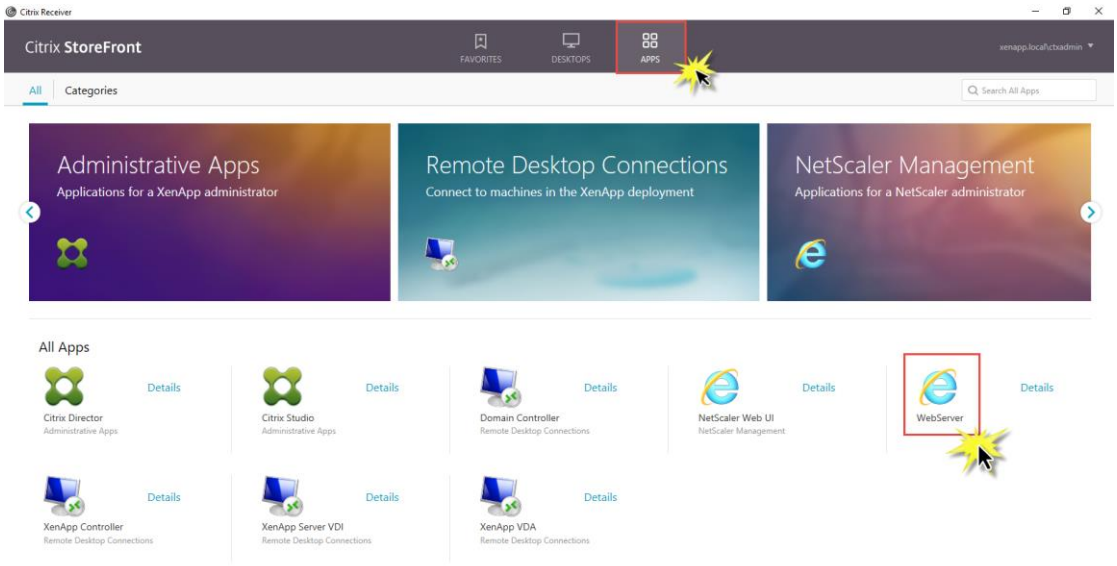
Εικόνα 4-6. Receiver Accounts

✓ Ο χρήστης τοποθετεί τα διαπιστευτήρια του



Εικόνα 4-7. Receiver Credentials

✓ Αφού ταυτοποιηθεί επιτυχώς ο χρήστης περιηγείται μέσω των καρτελών Desktops και Apps στις εφαρμογές που είναι διαθέσιμες για τον λογαριασμό του και επιλέγει την εφαρμογή που επιθυμεί

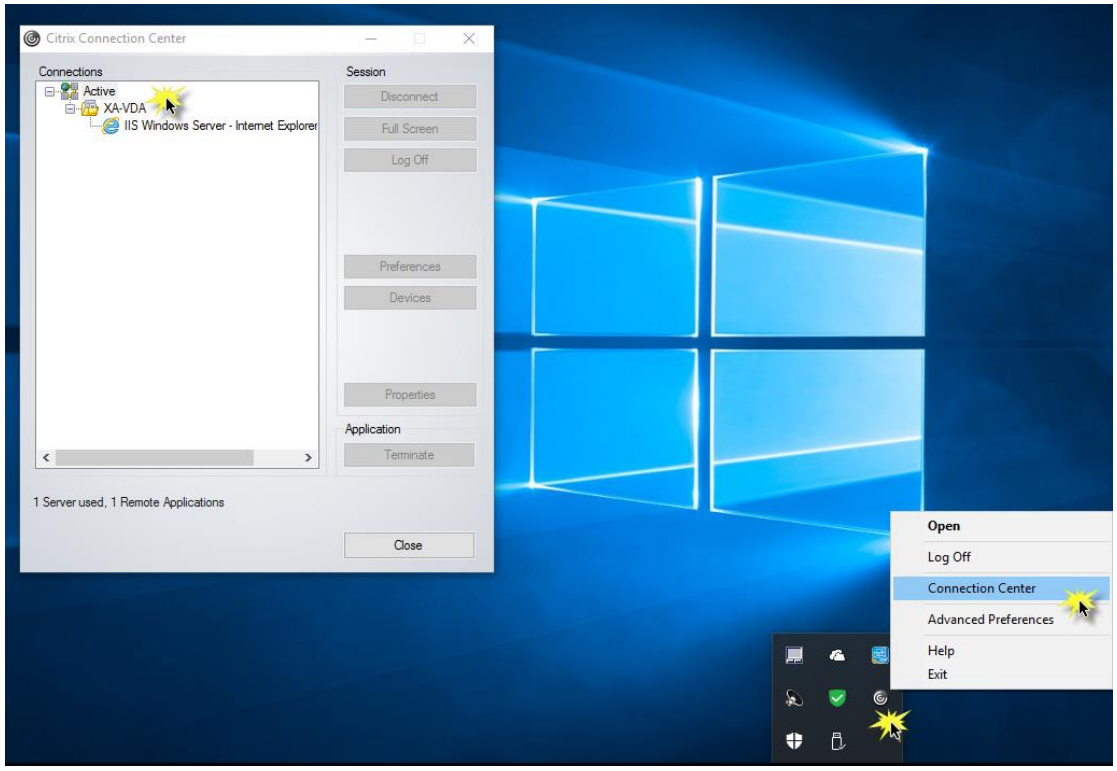


Εικόνα 4-8. Receiver Apps

✓ Εκτελείται η εφαρμογή που επέλεξε ο χρήστης

Εικόνα 4-9. XenApplication

- ✓ Στην παρακάτω εικόνα φαίνεται ποιος XenApp server εξυπηρετεί τον χρήστη

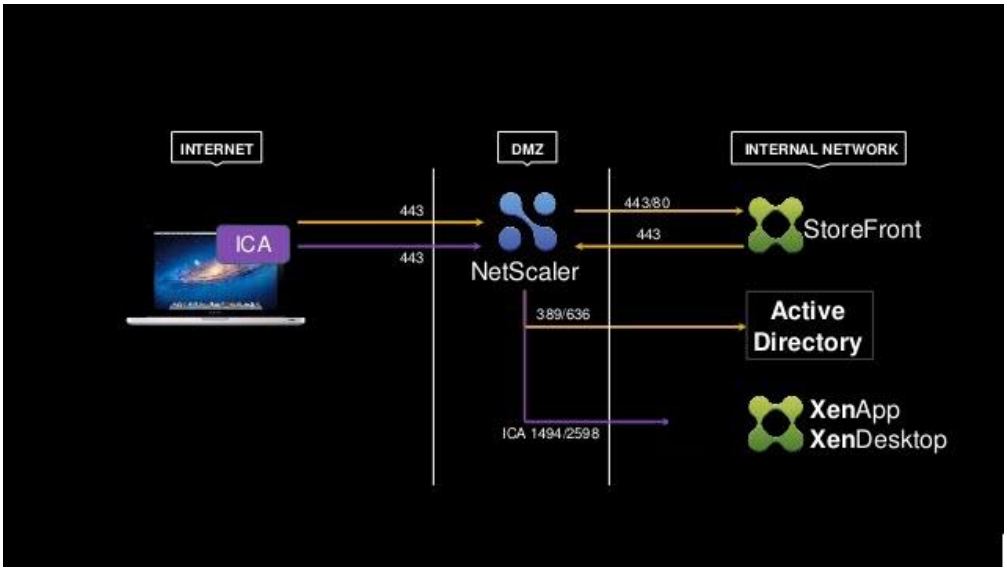


Εικόνα 4-10. Connection Center

Η παραπάνω διαδικασία μπορεί να αποδοθεί λεπτομερειακά, αναφέροντας όλα τα μέρη της υποδομής που συμμετέχουν στην αλληλεπίδραση χρήστη-συστήματος:

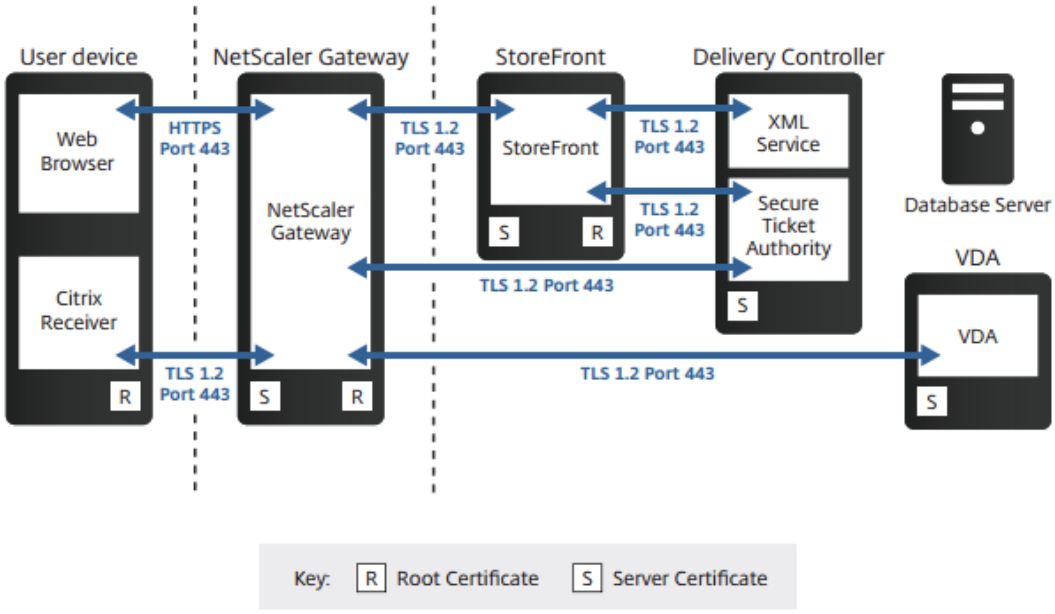
- ✓ Η επικοινωνία SSL ξεκινά καθώς ο χρήστης εκτελεί τον citrix receiver, ο οποίος χρησιμοποιεί το URL του Netscaler για να επικοινωνήσει μαζί του

- ✓ Ο χρήστης χρησιμοποιεί τα διαπιστευτήρια του τα οποία αποστέλλονται στον Netscaler, ο οποίος με την σειρά του επικοινωνεί με τον Domain Controller (ή LDAP) για να γίνει η ταυτοποίηση
- ✓ Αφού ολοκληρωθεί η ταυτοποίηση του χρήστη ο Netscaler αποστέλλει τα στοιχεία του χρήστη στον Storefront ο οποίος τα προωθεί στον Datacollector ο οποίος επικυρώνει τον χρήστη μέσω του Domain Controller (ή LDAP) όσο αφορά την λίστα των εφαρμογών στις οποίες ο χρήστης έχει πρόσβαση η οποία αποστέλλεται πίσω στον Storefront
- ✓ Ο Storefront επιστρέφει την πληροφορία στον Netscaler η οποία καταλήγει στον χρήστη ο οποίος βλέπει τις εφαρμογές που είναι διαθέσιμες σε αυτόν μέσω του citrix receiver
- ✓ Ο χρήστης επιλέγει ποια εφαρμογή θα εκτελεστεί, η πληροφορία αποστέλλεται στον Netscaler ο οποίος την προωθεί στον Storefront
- ✓ Ο Storefront επικοινωνεί με τον Datacollector ο οποίος αποφασίζει ποιος XenApp server έχει τον λιγότερο φόρτο και μπορεί να σερβίρει την εφαρμογή, έπειτα ο Datacollector (STA) επιστρέφει ένα ticket (το οποίο θα χρησιμοποιηθεί για να αναγνωριστεί ο XA server) στον Storefront ο οποίος προσθέτει αυτήν την πληροφορία στο ICA file και το προωθεί στον Netscaler
- ✓ Ο Netscaler στέλνει το αρχείο στον χρήστη ο οποίος εκτελεί το αρχείο μέσω αυτοματοποιημένης διαδικασίας
- ✓ Έπειτα ξεκινά μία νέα επικοινωνία SSL μέσω του Netscaler ο οποίος επικοινωνεί με τον Datacollector (STA) από τον οποίο στάλθηκε το ticket και ο οποίος στέλνει τις λεπτομέρειες που αφορούν τον XenApp server (IP address, port, hostname, application name)
- ✓ Ο Netscaler ξεκινά μια νέα επικοινωνία ICA με τον XenApp server και έπειτα λειτουργεί σαν ενδιάμεσος proxy server σε όλη την διάρκεια της επικοινωνίας μεταξύ χρήστη και XenApp server



Εικόνα 4-11. Netscaler as Proxy

- ✓ Οι παραπάνω επικοινωνίες εκτελούνται μέσω πρωτοκόλλων ασφαλείας SSL και TLSv2 σε όλα τα επίπεδα, τόσο στο εσωτερικό δίκτυο όσο και στο σημείο όπου παρεμβάλλεται το διαδίκτυο, όπως επίσης και η χρήση πιστοποιητικών ασφαλείας είναι απαραίτητη.

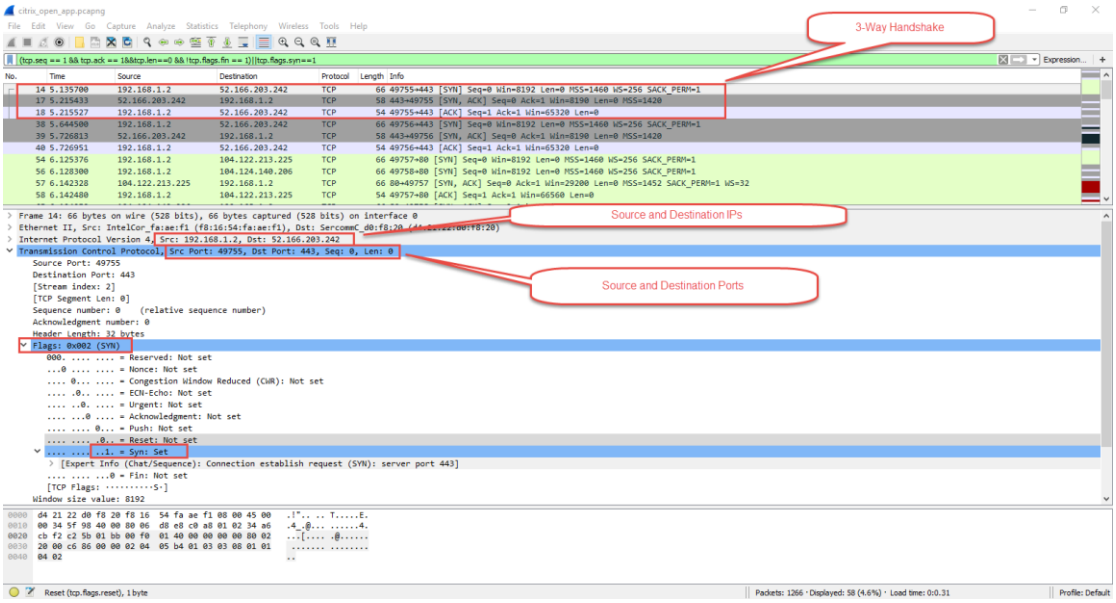


Εικόνα 4-12. Communication Secure Protocols

4.1.4 *Χρήση Wireshark κατά την διαδικασία χρήσης XenApplication (ICA file)*

Η διαδικασία εκτέλεσης μιας εφαρμογής Citrix μπορεί να αναλυθεί περαιτέρω με την χρήση του προγράμματος WireShark, στην πρώτη εικόνα απεικονίζεται η μέθοδος “3 Way Handshake” που χρησιμοποιείται για να δημιουργηθεί η σύνδεση μεταξύ server και client χρησιμοποιώντας πακέτα SYN και ACK.

- ✓ Ο client αποστέλλει ένα πακέτο SYN στον Netscaler ρωτώντας αν είναι διαθέσιμος για νέες συνδέσεις
- ✓ Ο Netscaler απαντάει με ένα SYN/ACK πακέτο δηλώνοντας την διαθεσιμότητα του
- ✓ Ο client λαμβάνει το πακέτο και απαντά με ένα ACK για να ξεκινήσει η σύνδεση



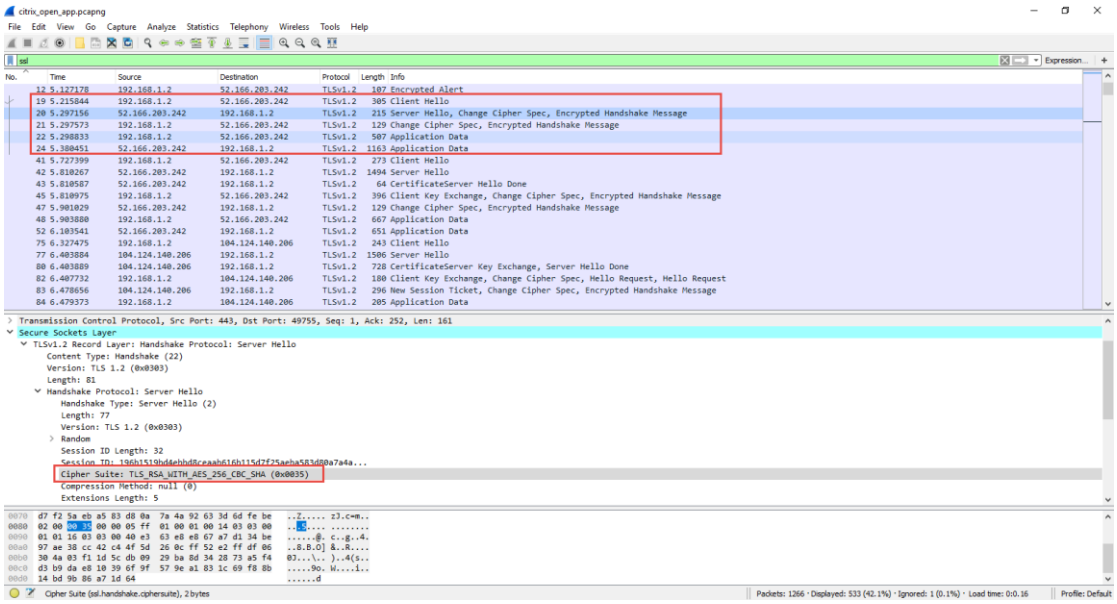
Εικόνα 4-13. 3 Way Handshake

Μετά την εγκαθίδρυση της επικοινωνίας λαμβάνει μέρος η διαδικασία επικοινωνίας των δύο πλευρών μέσω ασφαλής σύνδεσης, κάνοντας χρήση του πρωτοκόλλου TLSv1.2.

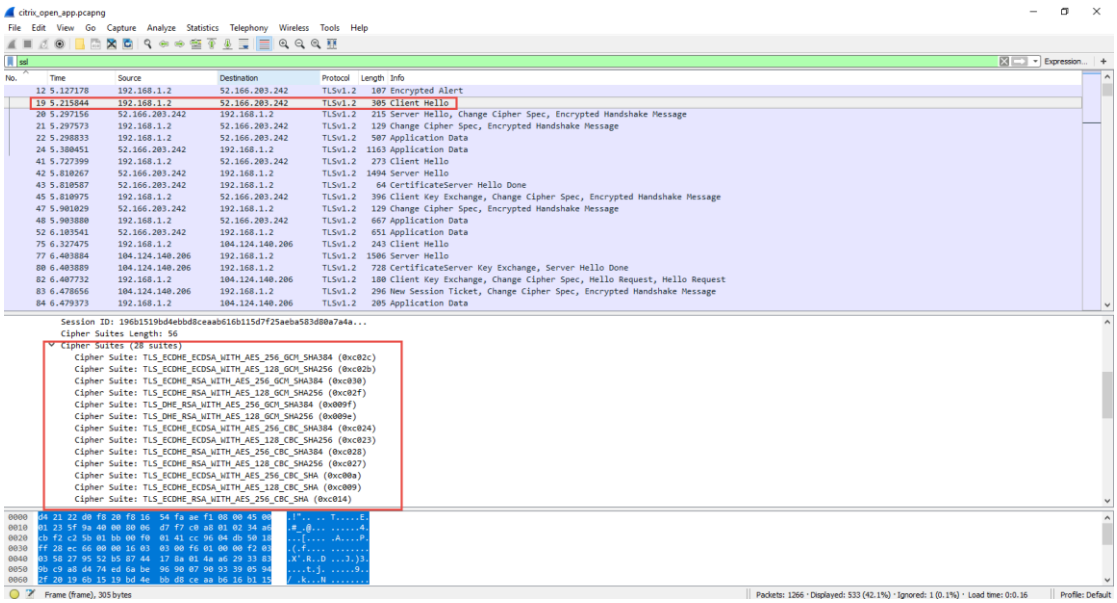
- ✓ Ο client αποστέλλει ένα “hello” μήνυμα διαφημίζοντας τους κρυπτογραφικούς αλγόριθμους που χρησιμοποιεί
- ✓ Ο server απαντά επιλέγοντας τον αλγόριθμο που θα χρησιμοποιηθεί
- ✓ Στο πεδίο Random διακρίνουμε τα “random bits” που αποστέλλονται και από τις δύο πλευρές. Με αυτόν τον τρόπο γίνεται μοναδική η επικοινωνία μεταξύ των δύο πλευρών και αποφεύγονται οι επιθέσεις “replay” κατά τις οποίες

δεδομένα παλαιότερων συνδέσεων χρησιμοποιούνται για να διασπαστεί η τρέχουσα επικοινωνία.

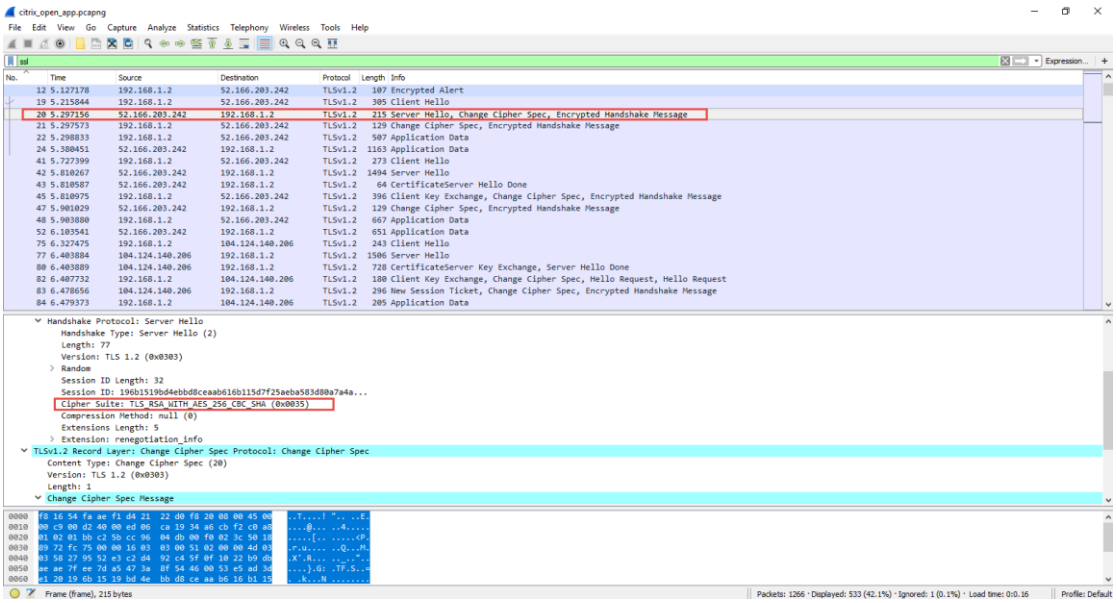
- ✓ Τέλος χρησιμοποιείται ένα “Session ID” έτσι ώστε να είναι αποτελεσματικότερη η επανασύνδεση σε περίπτωση που ο client κλείσει την επικοινωνία και επικοινωνήσει ξανά στο κοντινό μέλλον.



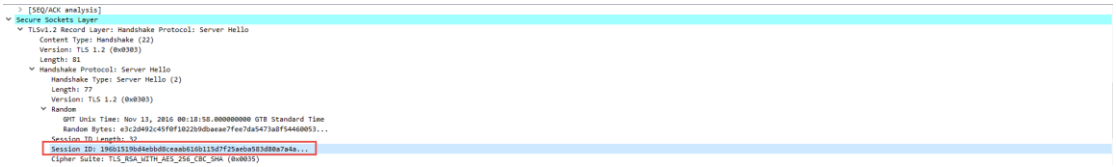
Εικόνα 4-14. Cipher Specs



Εικόνα 4-15. Client’s Hello



Εικόνα 4-16. Netscaler's Hello



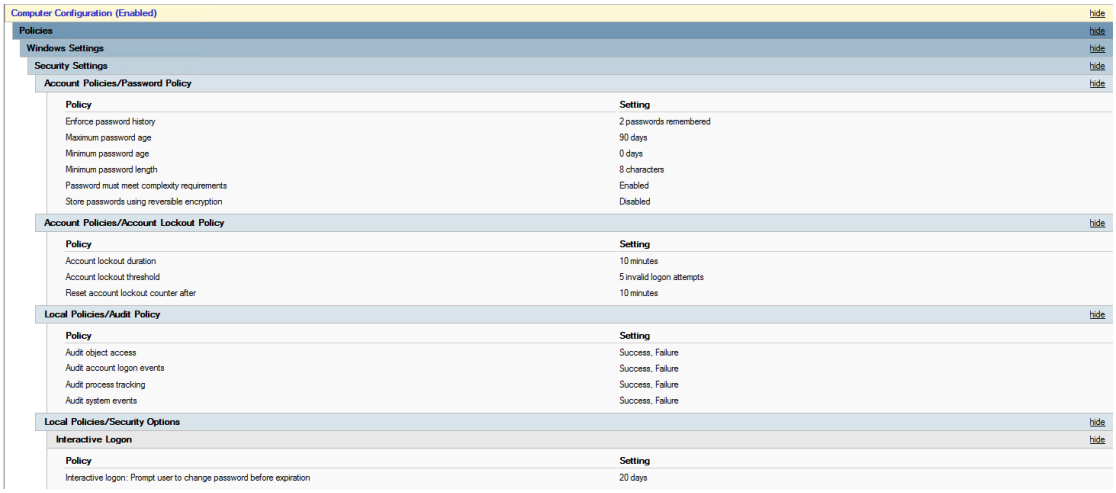
Εικόνα 4-17. Random-Session ID

4.2 Ενδυνάμωση περιβάλλοντος Citrix

Η ασφάλεια είναι ένα από τα σημαντικότερα θέματα που μας απασχολεί σε μια τέτοια υποδομή. Παρακάτω θα εφαρμόσουμε κανόνες και πολιτικές ασφαλείας σε όλα τα μέρη της υποδομής καθώς μόνο με αυτόν τον τρόπο μπορεί να επέλθει ένα ικανοποιητικό επίπεδο ασφαλείας συνολικά στην υποδομή.

4.2.1 Πολιτικές Domain Controller

Μπορούμε να εφαρμόσουμε πολιτικές ασφαλείας, τόσο Domain-policies όσο και Citrix-policies έτσι ώστε να περιορίσουμε τα κενά ασφαλείας σύμφωνα με τις ανάγκες μας. Στο παρακάτω παράδειγμα διακρίνουμε μία domain πολιτική η οποία θέτει παραμέτρους για τα password των χρηστών του domain αλλά και ρυθμίσεις auditing.



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	2 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout duration	10 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	10 minutes

Local Policies/Audit Policy hide

Policy	Setting
Audit object access	Success, Failure
Audit account logon events	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Local Policies/Security Options hide

Interactive Logon hide

Policy	Setting
Interactive logon: Prompt user to change password before expiration	20 days

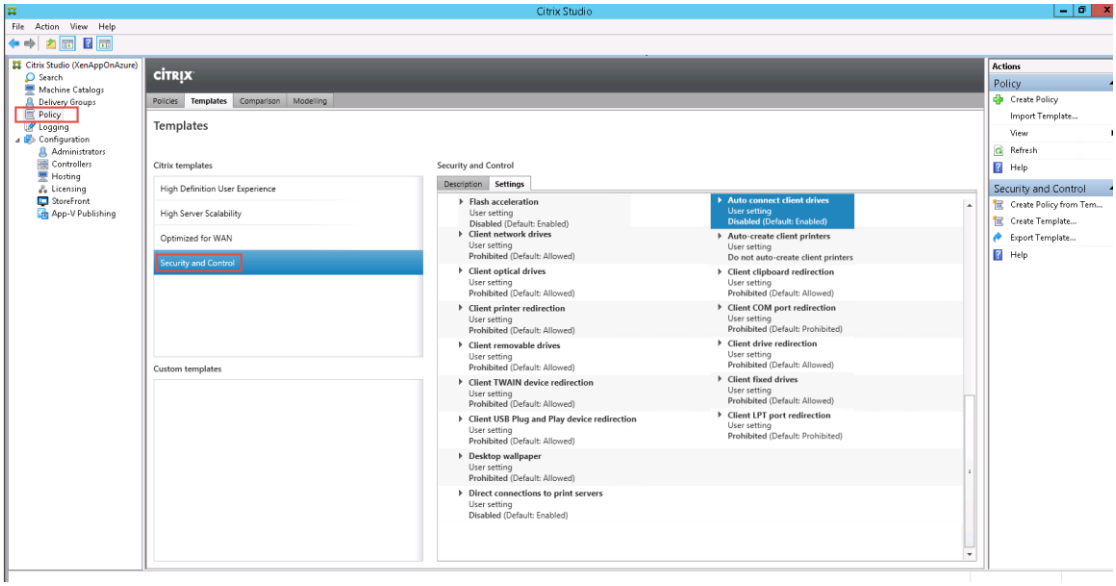
Εικόνα 4-18. Domain Policy

4.2.2 Πολιτικές Citrix

Μέσω της κονσόλας Citrix Studio είναι δυνατή η δημιουργία πολιτικών αλλά και η ρύθμιση default πολιτικών όπως φαίνεται στην παρακάτω εικόνα.

Οι σημαντικότερες επιλογές πολιτικών ασφαλείας είναι:

- Client removable devices, όπου με την επιλογή “Prohibited” απαγορεύει στον χρήστη την μεταφορά αρχείων από τον τοπικό client στο περιβάλλον Citrix μέσω αφαιρούμενων συσκευών όπως usb sticks.
- Client clipboard redirection, όπου με την επιλογή “Prohibited” απαγορεύει στον χρήστη την αντιγραφή-επικόλληση αρχείων από τον τοπικό client στο περιβάλλον Citrix.
- Client Network drives, όπου με την επιλογή “Prohibited” δεν είναι δυνατή η μεταφορά-mapping των κοινόχρηστων στοιχείων δικτύου που πιθανόν υπάρχουν στον τοπικό client του χρήστη.
- Client Printer Redirection, όπου επιλέγοντας “Prohibited” απενεργοποιείται η δυνατότητα χρήσης των εκτυπωτικών μέσων που είναι συνδεδεμένοι στο τοπικό μηχάνημα του χρήστη, στο περιβάλλον Citrix. Τα εκτυπωτικά αυτά μέσα ίσως είναι διαδικτυακά με αποτέλεσμα αν επιτραπεί η σύνδεση τους στο Citrix να δημιουργηθούν κενά ασφαλείας.



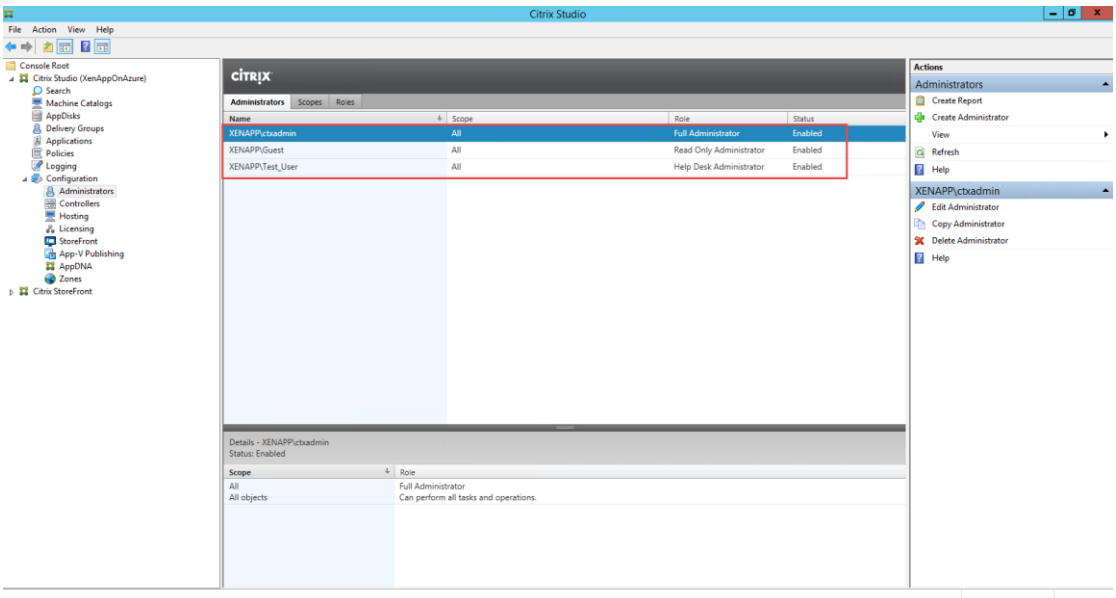
Εικόνα 4-19. Citrix Policies

Παρακάτω διακρίνονται οι ρόλοι των διαχειριστών της υποδομής Citrix:

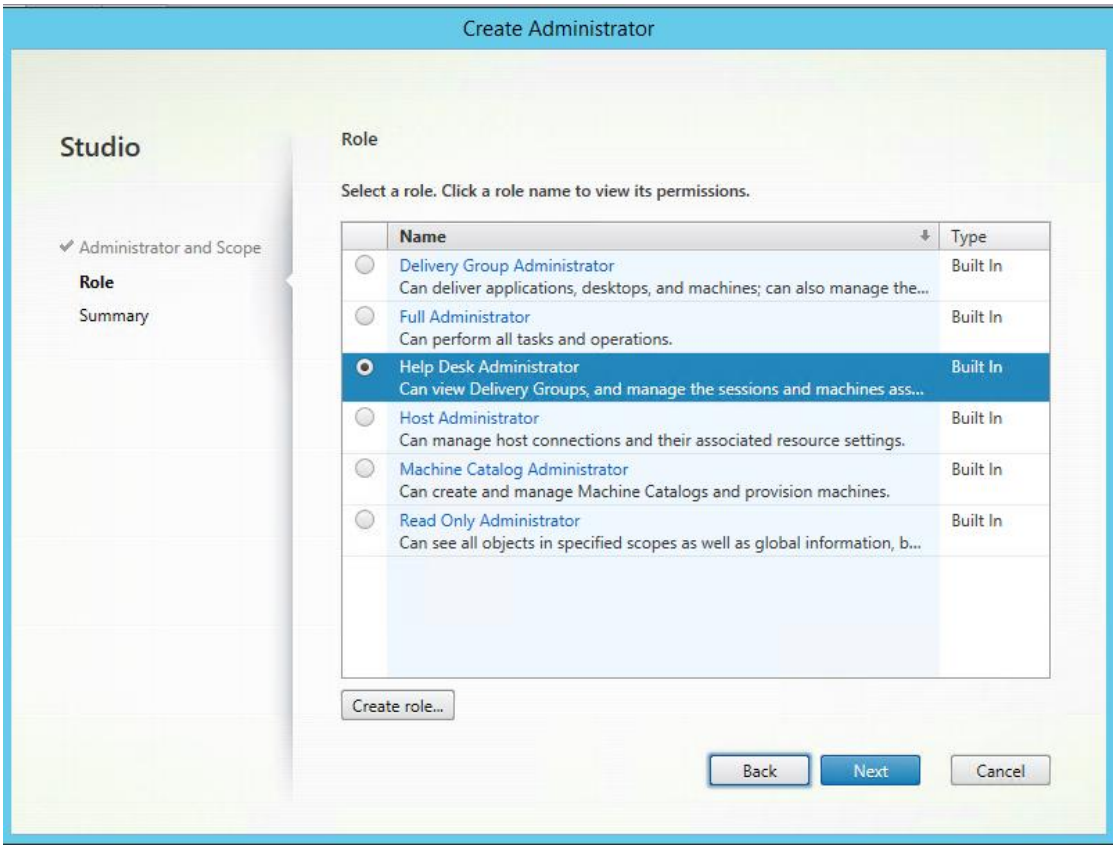
- ctxadmin, ο οποίος διαθέτει full administration δικαιώματα στις κονσόλες διαχείρισης Citrix studio, director και storefront

- test_user, ο οποίος διαθέτει δικαιώματα Helpdesk τα οποία περιορίζονται στις λειτουργίες logoff-restart των sessions και των VMs

- guest, χωρίς κανένα δικαίωμα παραμετροποίησης-αλλαγής ρυθμίσεων, παρά μόνο read-only για την παρακολούθηση της υποδομής



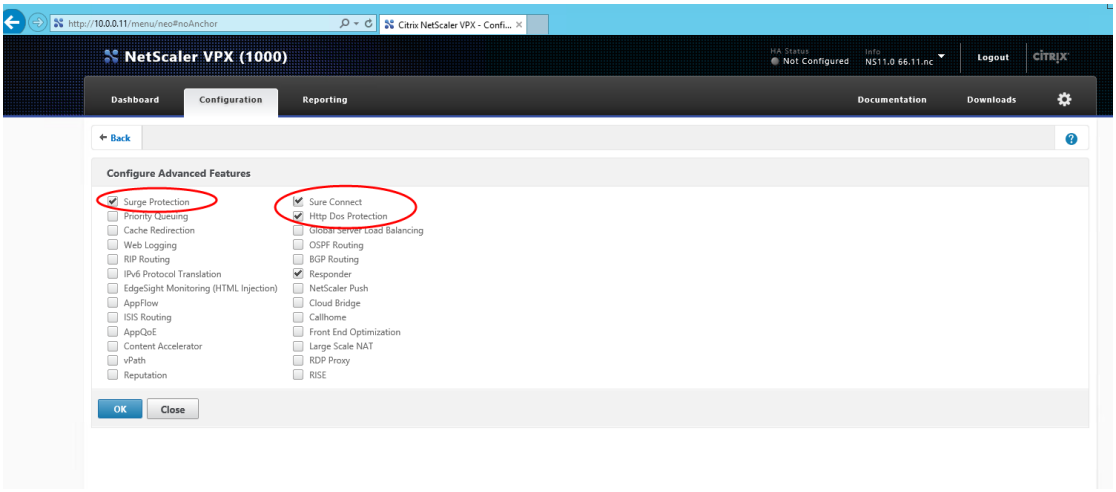
Εικόνα 4-20. Administration Roles



Εικόνα 4-21. Role creation

4.2.3 Netscaler Configuration

Το πιο σημαντικό κομμάτι για την προστασία του περιβάλλοντος Citrix από πιθανές επιθέσεις είναι η παραμετροποίηση και η χρήση μέτρων στον Netscaler μέσω των οποίων θα δημιουργήσουμε μία ασφαλέστερη υποδομή. Ξεκινώντας από βασικές ρυθμίσεις οι οποίες δεν πρέπει να παραλείπονται, ενεργοποιούμε τις επιλογές:



Εικόνα 4-22. Netscaler Settings

```
> enable ns feature surgeProtection
 Done
> enable ns feature httpDoSProtection
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   OFF
 2)     Surge Protection                SP                   ON
 3)     Load Balancing                  LB                   ON
 4)     Content Switching               CS                   ON
 5)     Cache Redirection               CR                   OFF
 6)     Sure Connect                    SC                   OFF
 7)     Compression Control             CMP                  OFF
 8)     Priority Queuing                PQ                   OFF
 9)     SSL Offloading                  SSL                  ON
 10)    Global Server Load Balancing    GSLB                 OFF
 11)    Http DoS Protection             HDOSP                ON
 12)    Content Filtering               CF                   OFF
 13)    Integrated Caching              IC                   OFF
 14)    SSL VPN                         SSLVPN               ON
 15)    AAA                             AAA                  ON
 16)    OSPF Routing                    OSPF                 OFF
 17)    RIP Routing                     RIP                  OFF
 18)    BGP Routing                     BGP                  OFF
 19)    Rewrite                         REWRITE              OFF
 20)    IPv6 protocol translation       IPv6PT               OFF
 21)    Application Firewall            AppFw                OFF
 22)    Responder                       RESPONDER            ON
 23)    HTML Injection                  HTMLInjection        OFF
 24)    NetScaler Push                  push                 OFF
 25)    AppFlow                         AppFlow              OFF
 26)    CloudBridge                     CloudBridge          OFF
 27)    ISIS Routing                    ISIS                 OFF
 28)    CallHome                        CH                   OFF
 29)    AppQoE                          AppQoE               OFF
 30)    vPath                           vPath                OFF
 31)    Content Accelerator             ContentAccelerator   OFF
 32)    RISE                            RISE                 OFF
 33)    Front End Optimization          FEO                  OFF
 34)    Large Scale NAT                 LSN                  OFF
 35)    RDP Proxy                       RDPProxy             OFF
 36)    Reputation                      Rep                  OFF
 Done
>
```

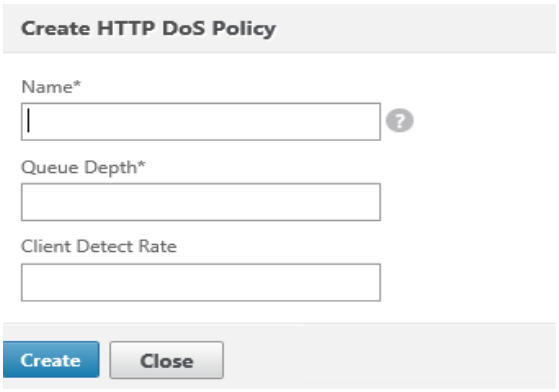
Εικόνα 4-23. Netscaler Settings via Command

- ✓ Surge protection, όπου καθορίζουμε πόσες συνδέσεις tcp μπορεί να διαχειριστεί ο server πριν ξεκινήσει να απορρίπτει πακέτα

Εικόνα 4-24. Surge

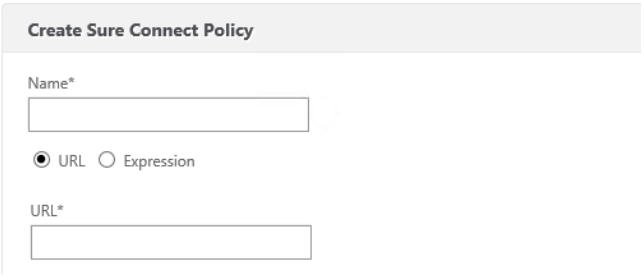
- ✓ Http DoS Protection, όπου καθορίζουμε το βάθος της ουράς και την αναλογία του client, που υποδηλώνουν το ποσοστό της κίνησης στο οποίο εφαρμόζεται η πολιτική Http Dos, η οποία όταν εφαρμοστεί αποστέλλεται μία πρόκληση

“JavaScript challenge” στον client, αν ο client απαντήσει με το σωστό cookie τότε η επικοινωνία επικυρώνεται.



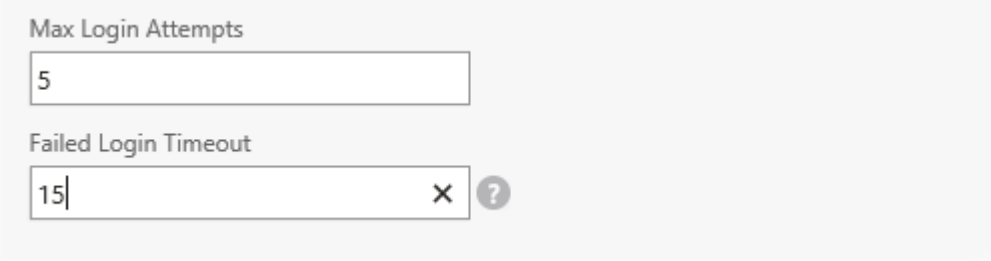
Εικόνα 4-25. Dos Policy

- ✓ Sure Connect, όπου δίνεται η δυνατότητα να οριστεί μία ενναλακτική σελίδα (web page) σε περίπτωση που οι “backend” δεν μπορούν να εξυπηρετήσουν τα αιτήματα



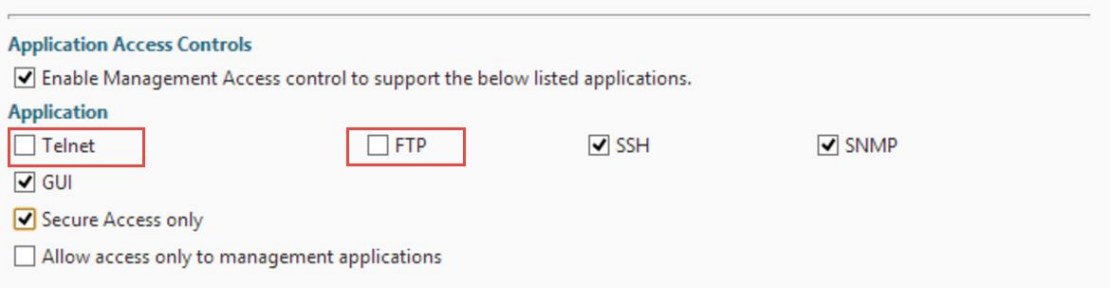
Εικόνα 4-26. Sure Connect

- ✓ Max login attempts and Failed login timeout, περιορίζουμε τις απόπειρες εισόδου των χρηστών (5 στο παρακάτω παράδειγμα) και επιλέγουμε το χρόνο (15 λεπτά) που ο χρήστης δεν θα έχει δικαίωμα πρόσβασης στο σύστημα αφού εξάντλησε το όριο των αποτυχημένων προσπαθειών που θέσαμε.



Εικόνα 4-27. Max Attempts

- ✓ Application Access Control, απενεργοποιούμε μεθόδους που δεν είναι απαραίτητες και μπορούν να δημιουργήσουν κενά ασφαλείας, όπως Telnet και FTP.

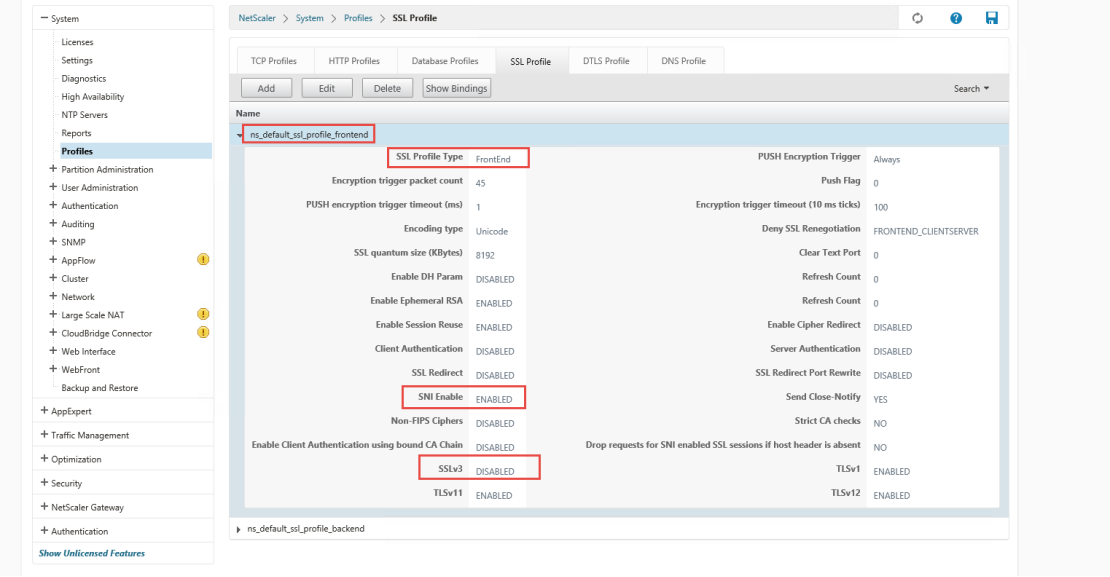


Εικόνα 4-28. AAC

Έπειτα από τις βασικές, ρυθμίζουμε το SSL προφίλ το οποίο μπορούμε και να εφαρμόσουμε σε όλους τους "Virtual Servers" αλλά κυρίως στον Netscaler:

1ο Βήμα

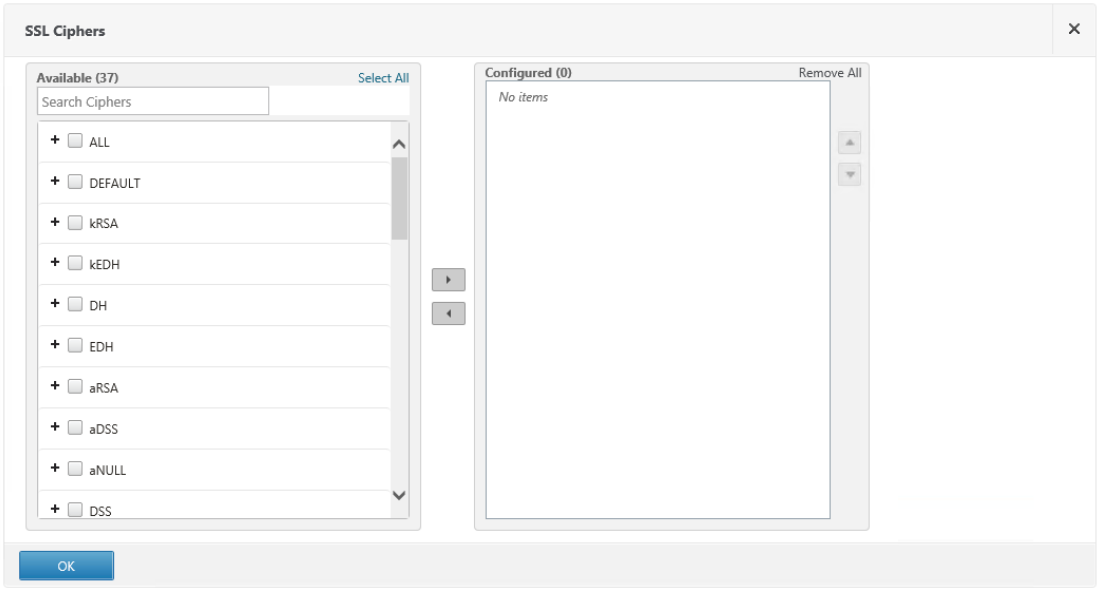
- ✓ Frontend profile, για να χρησιμοποιηθεί στους "Virtual Servers" για την διαχείριση των συνδέσεων των χρηστών
- ✓ SNI enable, για την χρήση πολλαπλών πιστοποιητικών για κάθε «Virtual Server"
- ✓ SSLv3 disable, η μη χρησιμοποίηση του πρωτοκόλλου βοηθά στην αποτροπή εκμετάλλευσης των αδυναμιών του



Εικόνα 4-29. SSL Profile

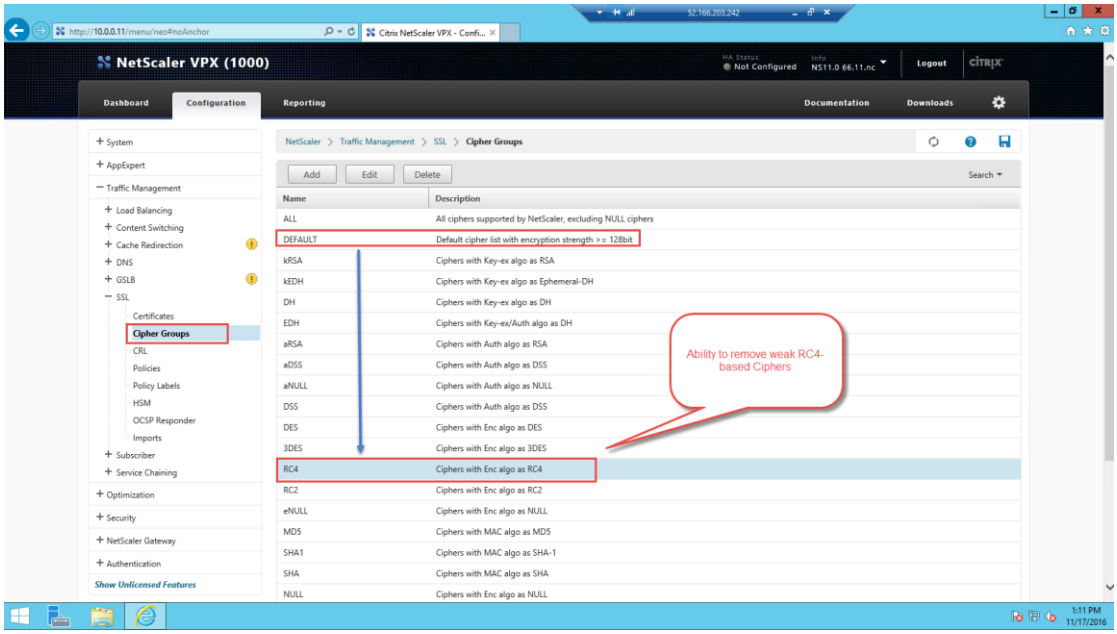
2ο Βήμα

- ✓ Επιλέγουμε τους κρυπτογραφικούς αλγόριθμους που θα χρησιμοποιηθούν



Εικόνα 4-30. Cipher Suites

- ✓ Μπορούμε να επιλέξουμε κάποιον από τις “default” επιλογές είτε να τις διαμορφώσουμε με τους αλγόριθμους που θέλουμε να χρησιμοποιήσουμε, όπως στο παρακάτω παράδειγμα όπου επιλέγουμε την “default” επιλογή έχοντας αφαιρέσει την δυνατότητα κρυπτογράφησής με RC4 αλγόριθμο που θεωρείται αδύναμος



Εικόνα 4-31. Default Suite

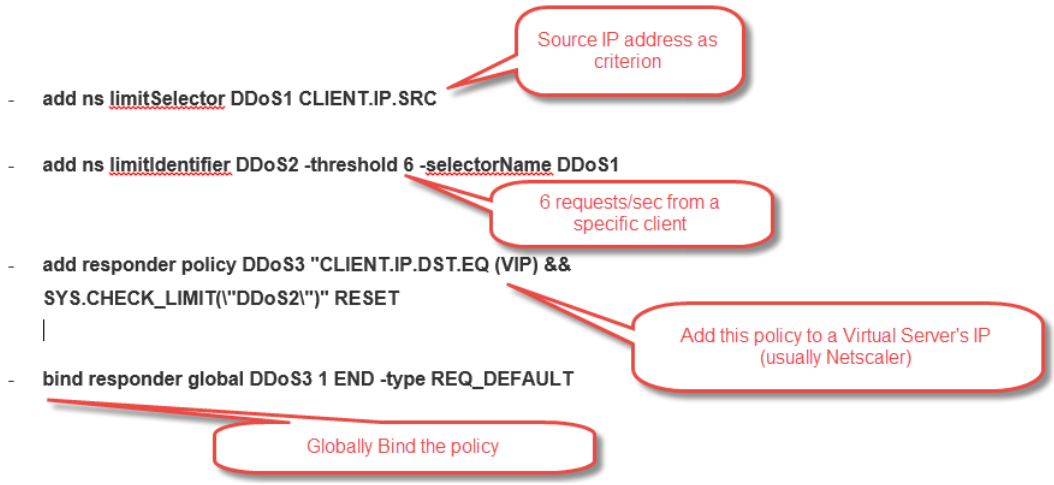
3ο Βήμα

- ✓ Εφαρμόζουμε το “SSL Profile” στους “Virtual Servers” που θέλουμε

Εικόνα 4-32. Bind Profile

Κανόνας αποφυγής επιθέσεων DDoS

Για να μετριάσουμε μία επίθεση DDoS ακολουθούμε την παρακάτω διαδικασία (με χρήση command line) με την οποία ρυθμίζουμε το όριο Rate, όταν αυτή η πολιτική εφαρμόζεται απορρίπτονται τα πακέτα αφού πρώτα έχει ξεπεραστεί το όριο που θέσαμε.

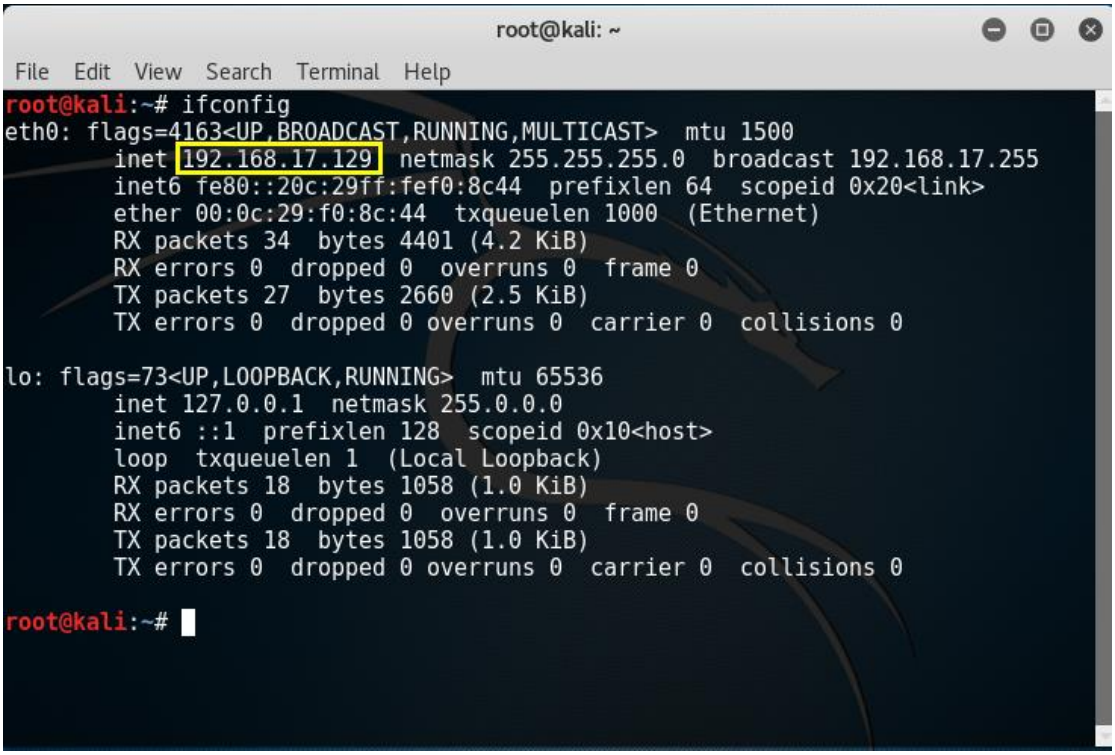


Εικόνα 4-33. DDoS Rule

4.3 Ανάπτυξη Σεναρίων Επιθέσεων

Τα παρακάτω είδη επιθέσεων εκτελέστηκαν μέσω λειτουργικού Kali-linux-2016.2

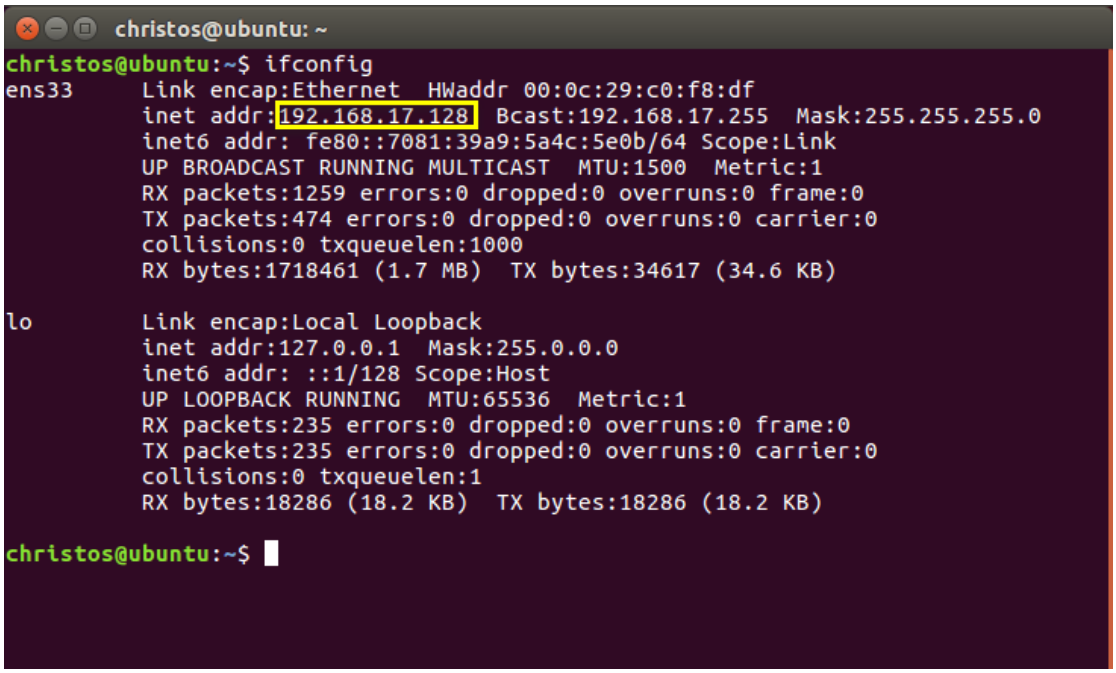
- ✓ Siege,
- ✓ slowloris,
- ✓ nping,



Εικόνα 4-34. Kali IP

Η παρακάτω επίθεση εκτελέστηκε μέσω λειτουργικού συστήματος Ubuntu-16.04.1

- ✓ LOIC

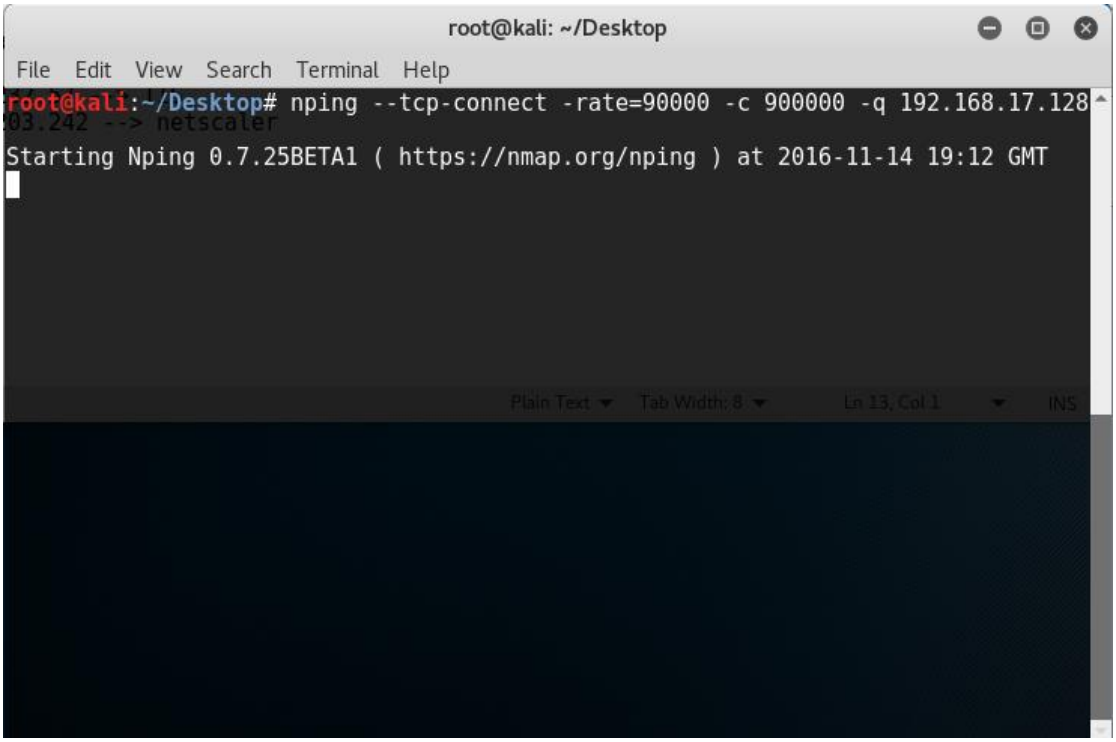


Εικόνα 4-35. Ubuntu IP

4.3.1 Επιθέσεις DDoS σε Apache2 – Λειτουργικό Σύστημα Ubuntu 16.04.1

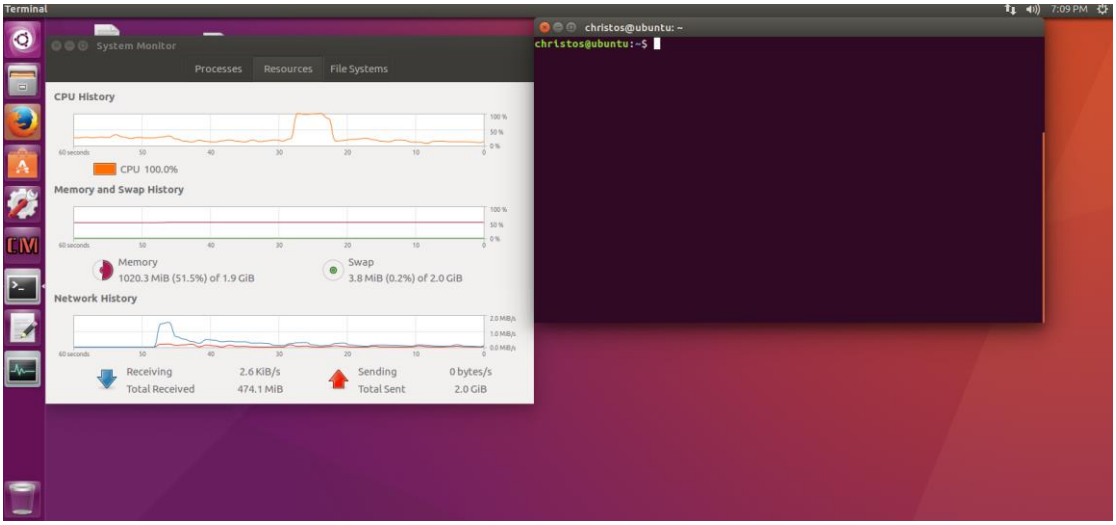
Επίθεση Nping

Εκτελείται με παραγωγή tcp πακέτων, αποστέλλοντας 90000πακέτα/δευτερόλεπτο (-rate) και ολοκληρώνεται μετά από 900000επαναλήψεις (-c) στον προορισμό με IP 192.168.17.128 (-q)



Εικόνα 4-36. Nping Attack

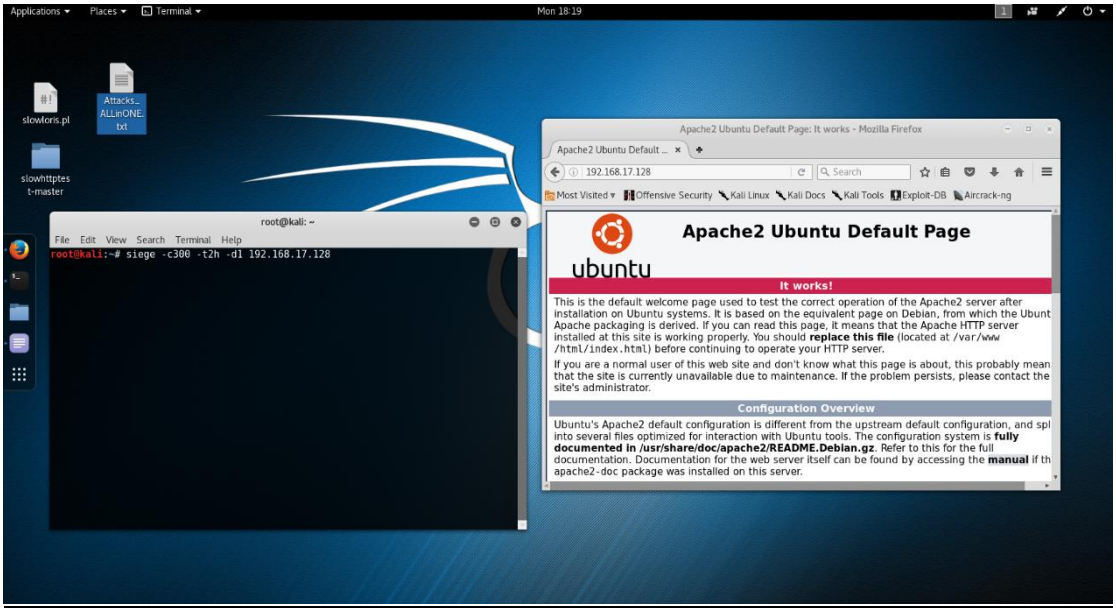
Η χρήση cpu αυξάνεται κατακόρυφα και η σελίδα είναι μη-διαθέσιμη μετά από 5 λεπτά.

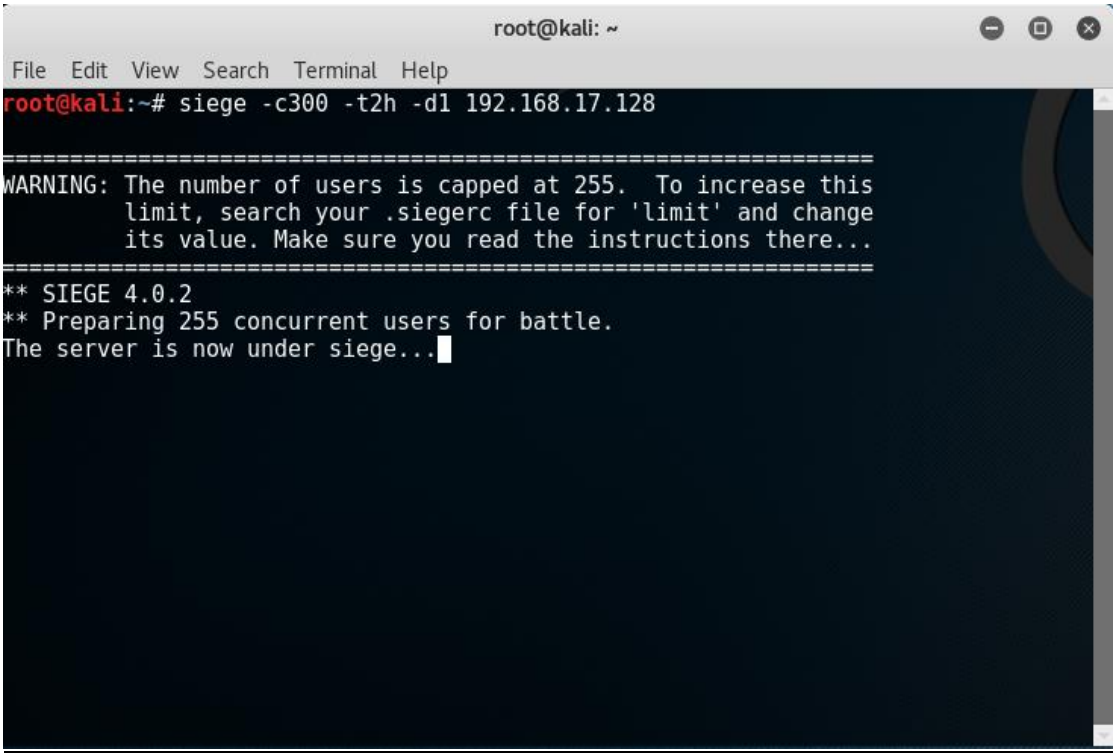


Εικόνα 4-37. CPU Usage

Επίθεση Siege

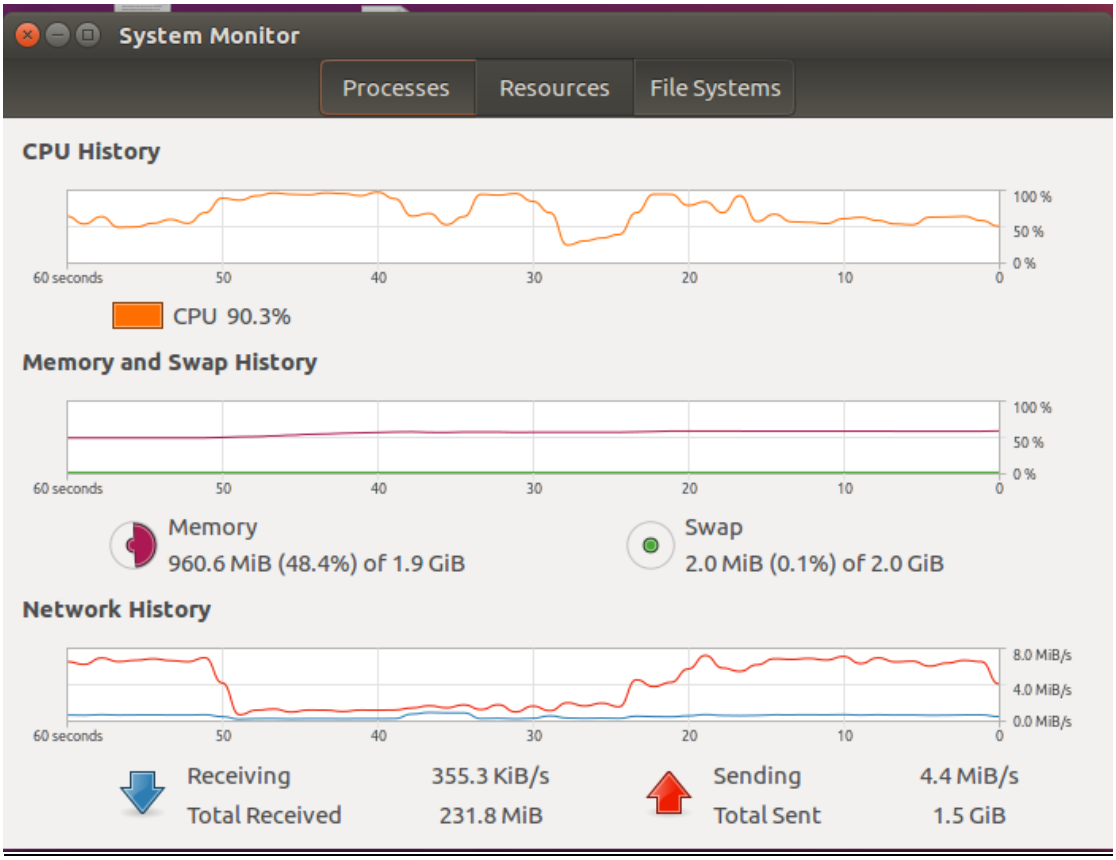
Εκτελείται προσομοιώνοντας 300χρήστες (-c) στην σελίδα, με χρονικό όριο 2 ώρες (-t) και χρόνο αναμονής μεταξύ των αιτημάτων 1δευτερόλεπτο (-d) στον προορισμό με IP 192.168.17.128



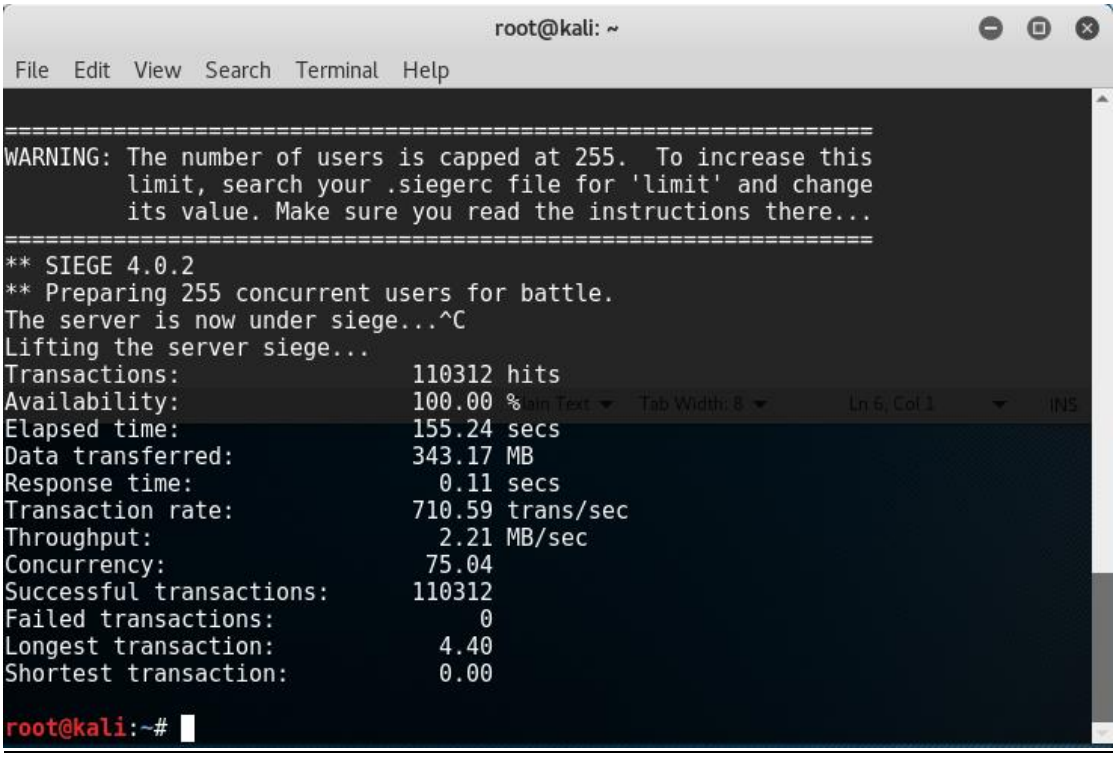


Εικόνα 4-38. Siege Attack

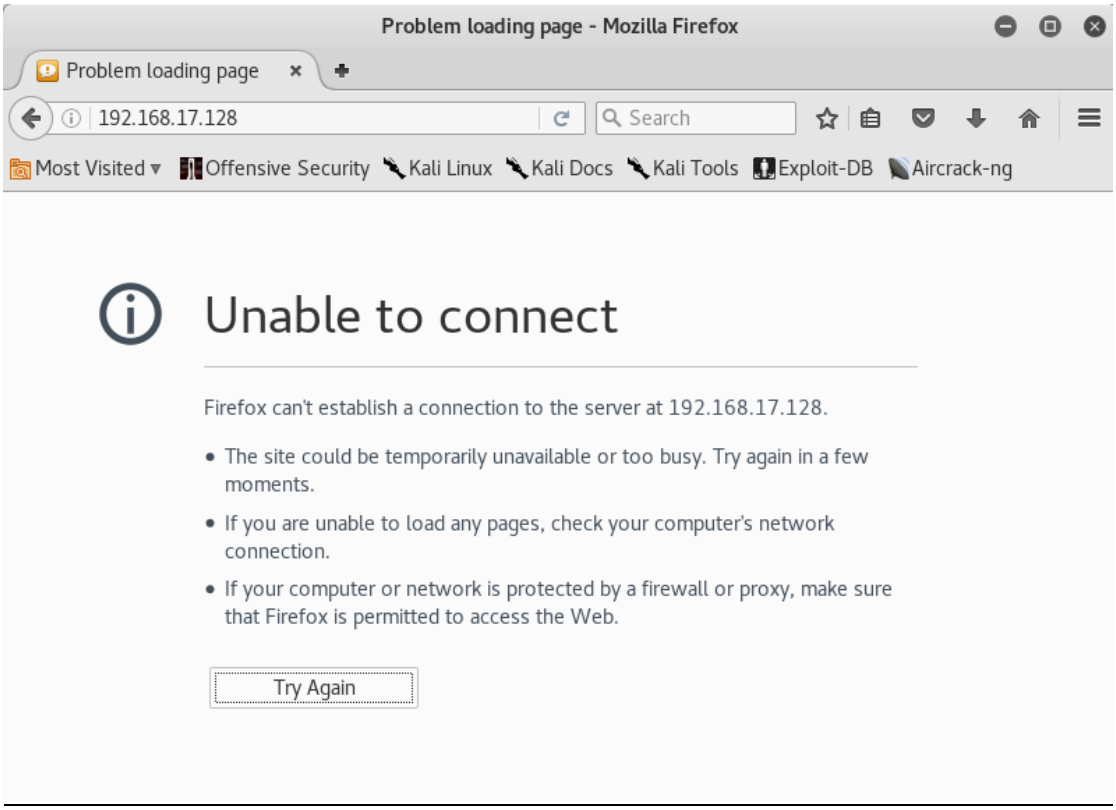
Όπως φαίνεται και παρακάτω ο φόρτος στον server είναι μεγάλος τόσο σε επίπεδο cpu όσο και network και σε 2,5 λεπτά η σελίδα είναι μη-διαθέσιμη.



Εικόνα 4-39. CPU Usage



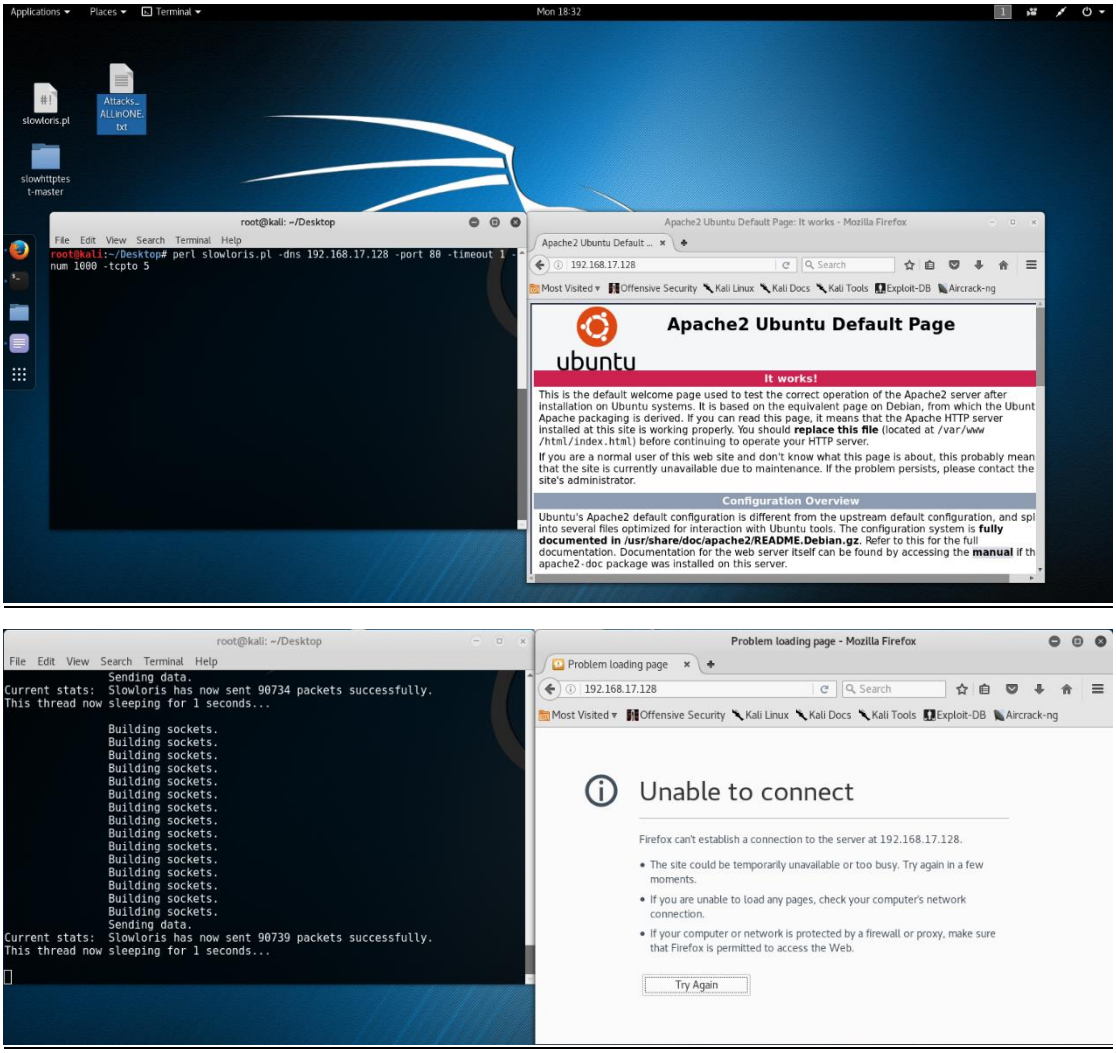
Εικόνα 4-40. Siege Results



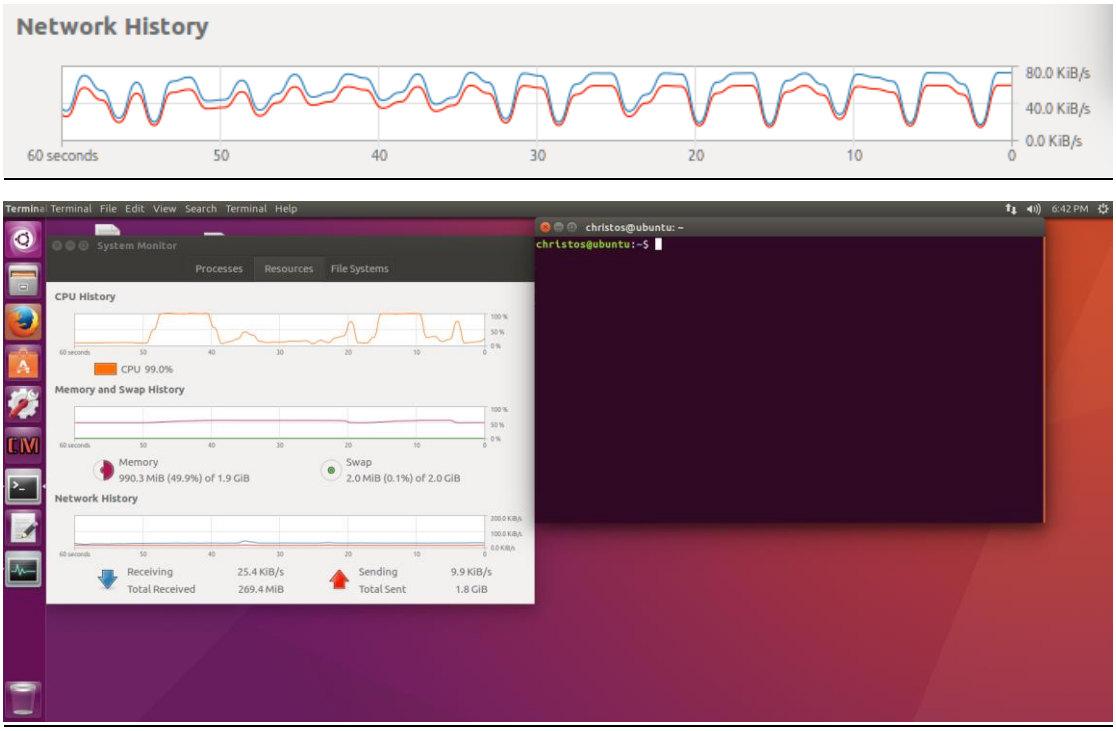
Εικόνα 4-41. Site Unavailability

Επίθεση Slowloris

Εκτελείται δημιουργώντας 1000συνδέσεις/δευτερόλεπτο (-num, -timeout) στην πόρτα 80 του προορισμού με IP 192.168.17.128, με αποτέλεσμα η σελίδα να μην είναι διαθέσιμη έπειτα από 2 λεπτά.



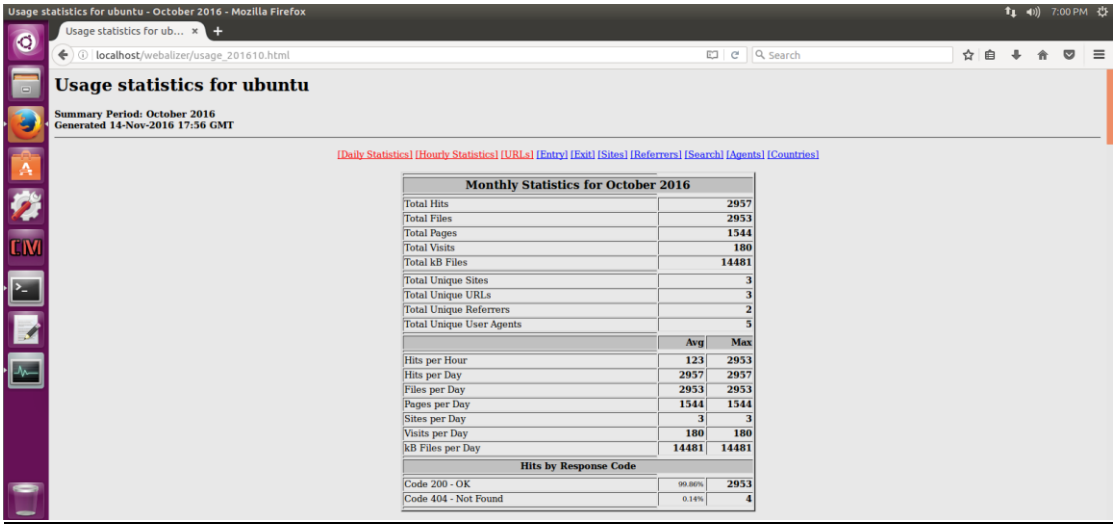
Εικόνα 4-42. Slowloris Attack

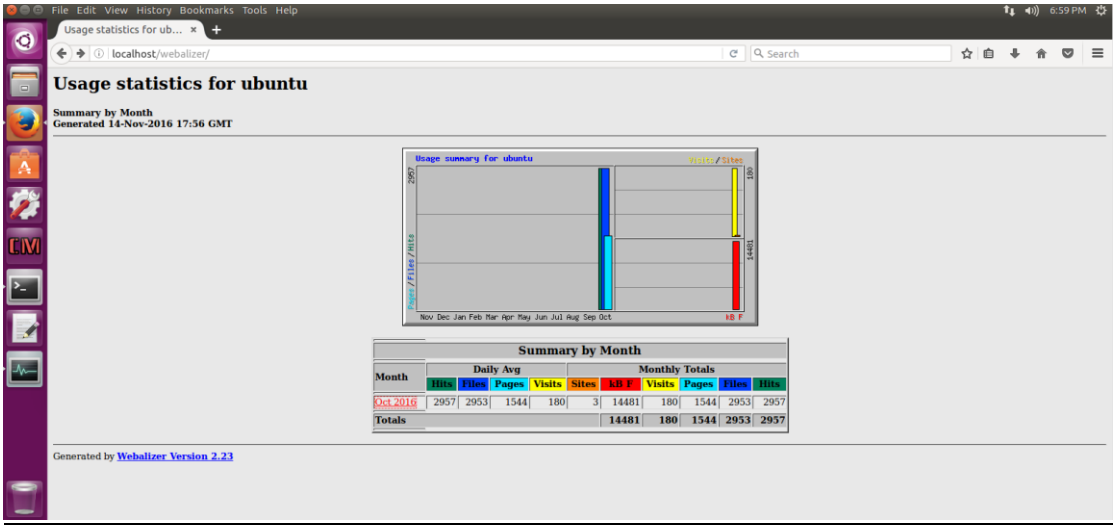


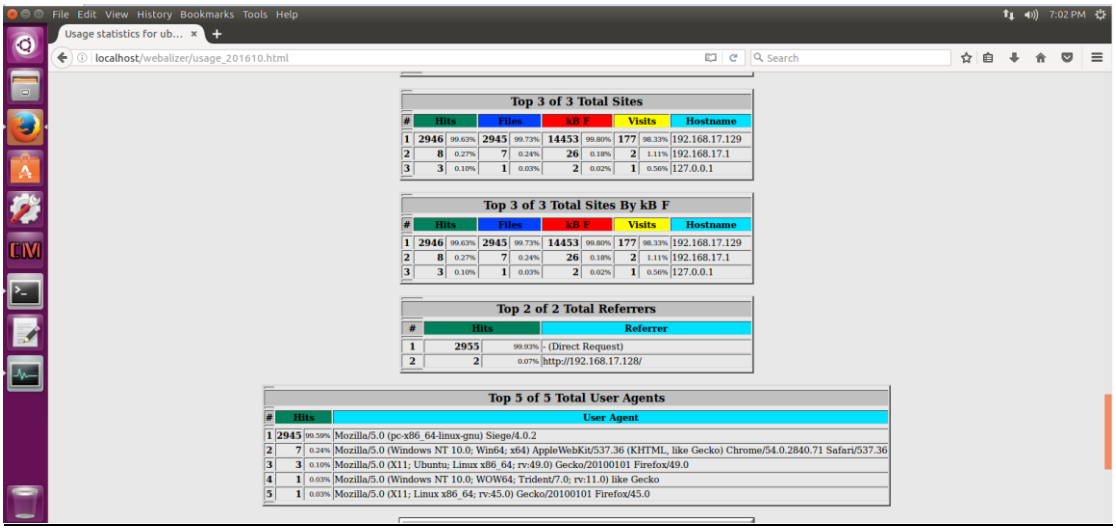
Εικόνα 4-43. Usage

Ανάλυση του log αρχείου του συστήματος

Χρησιμοποιώντας το εργαλείο Webalyzer παίρνουμε τα παρακάτω αποτελέσματα σχετικά με τα “requests” που είχε ο webserver κατά την διάρκεια των επιθέσεων.





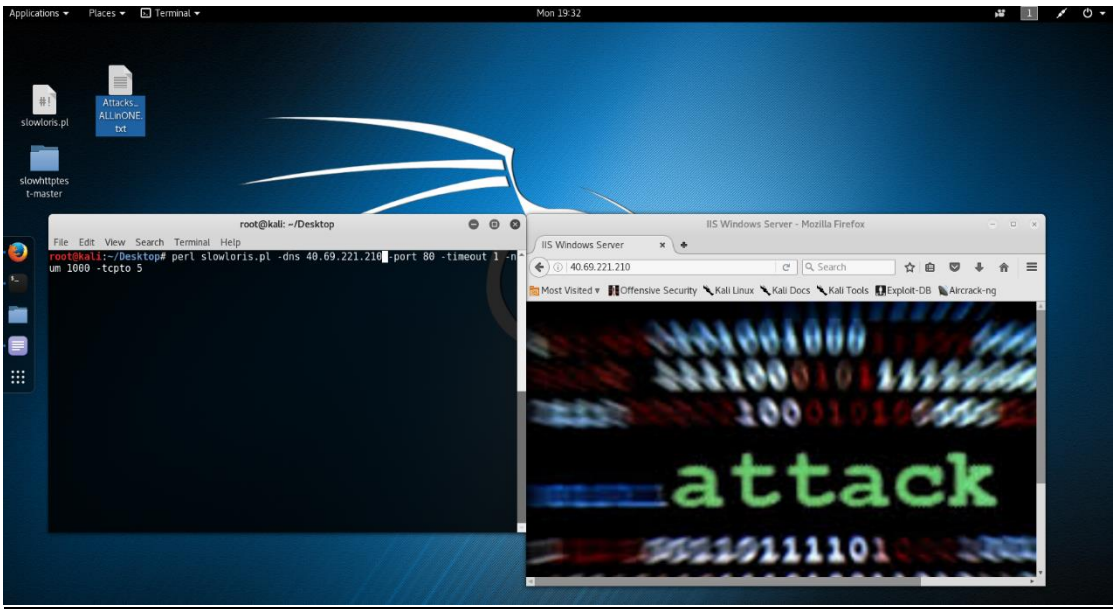


Εικόνα 4-44. Webalyzer Analysis

4.3.2 Επιθέσεις DDoS σε IIS 8.0 – Λειτουργικό Σύστημα Windows Server 2012R2

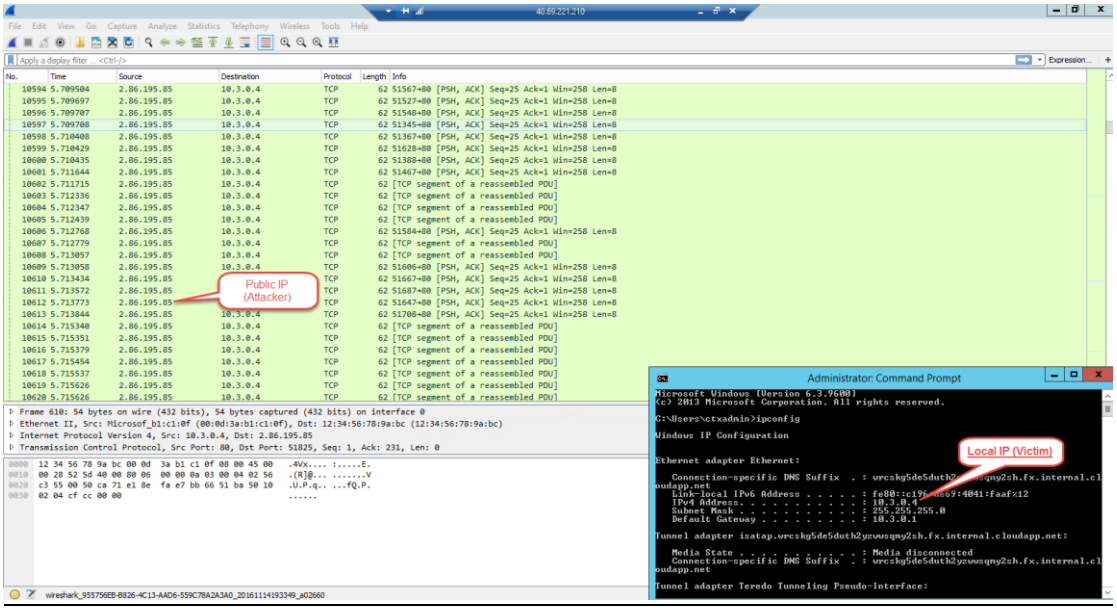
Επίθεση Slowloris

Η επίθεση εκτελείται με τα ίδια χαρακτηριστικά που εκτελέστηκε και προηγουμένως σε apache server με προορισμό την public IP του Windows webserver 40.69.221.210.



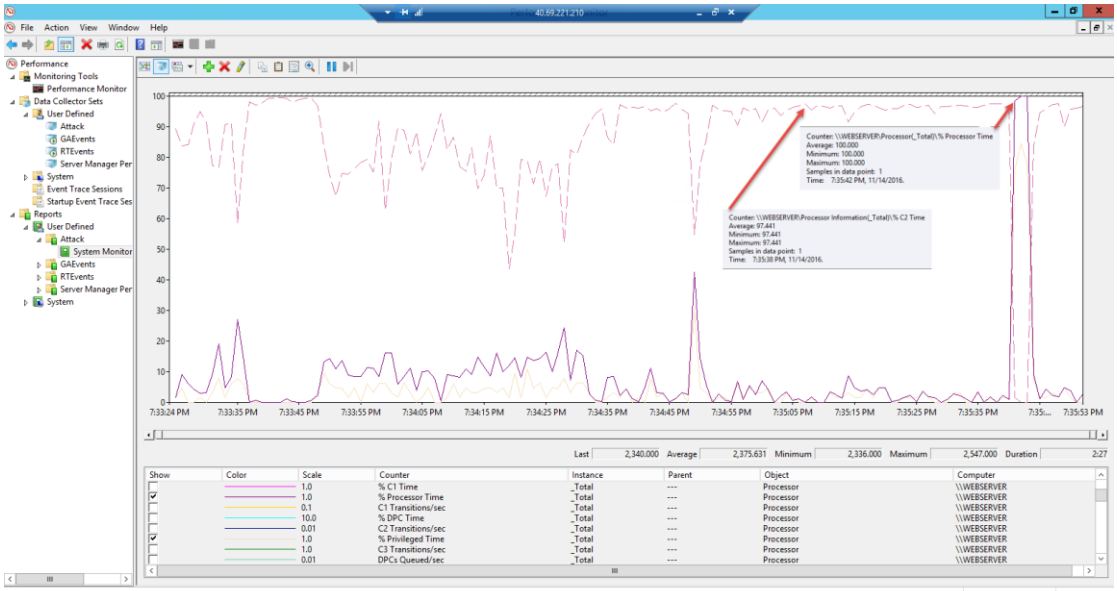
Εικόνα 4-45. Slowloris Attack

Με την χρήση wireshark βλέπουμε τα πακέτα tcp που δέχεται το θύμα της επίθεσης.

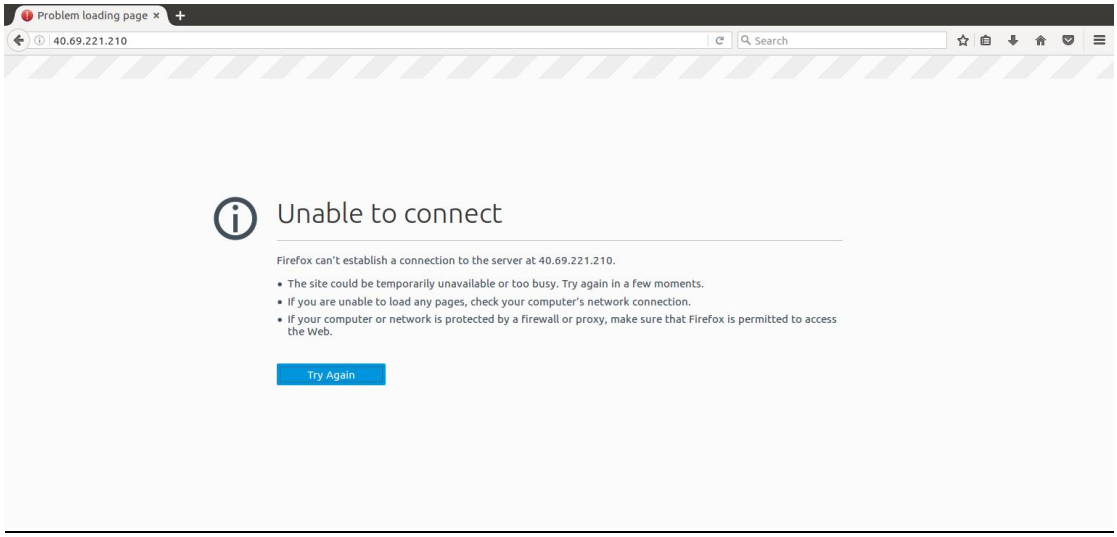


Εικόνα 4-46. WireShark Capture

Η cpu επηρεάζεται κατακόρυφα και σε 4 λεπτά η σελίδα είναι μη διαθέσιμη.



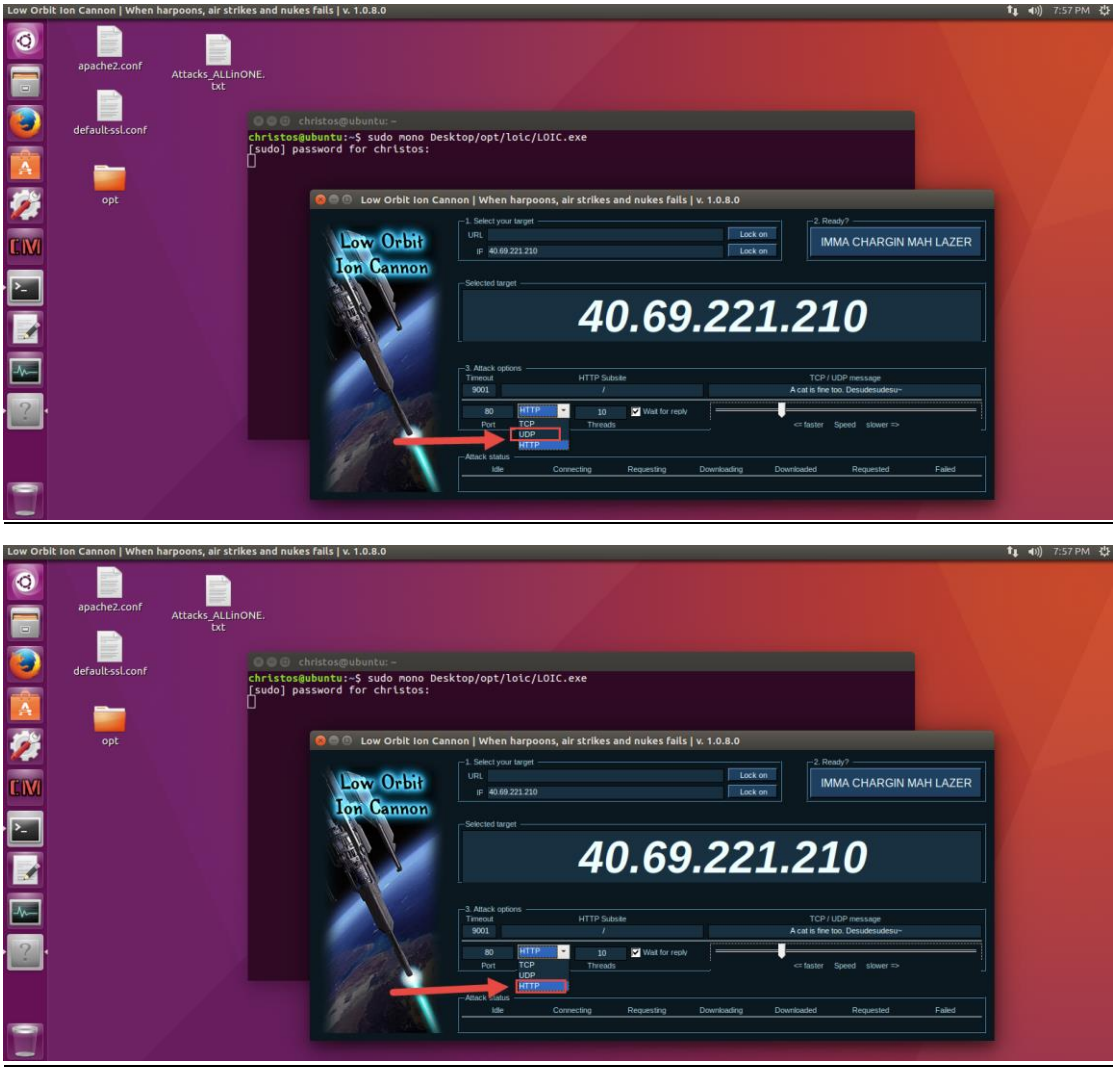
Εικόνα 4-47. CPU Usage



Εικόνα 4-48. Site Unavailability

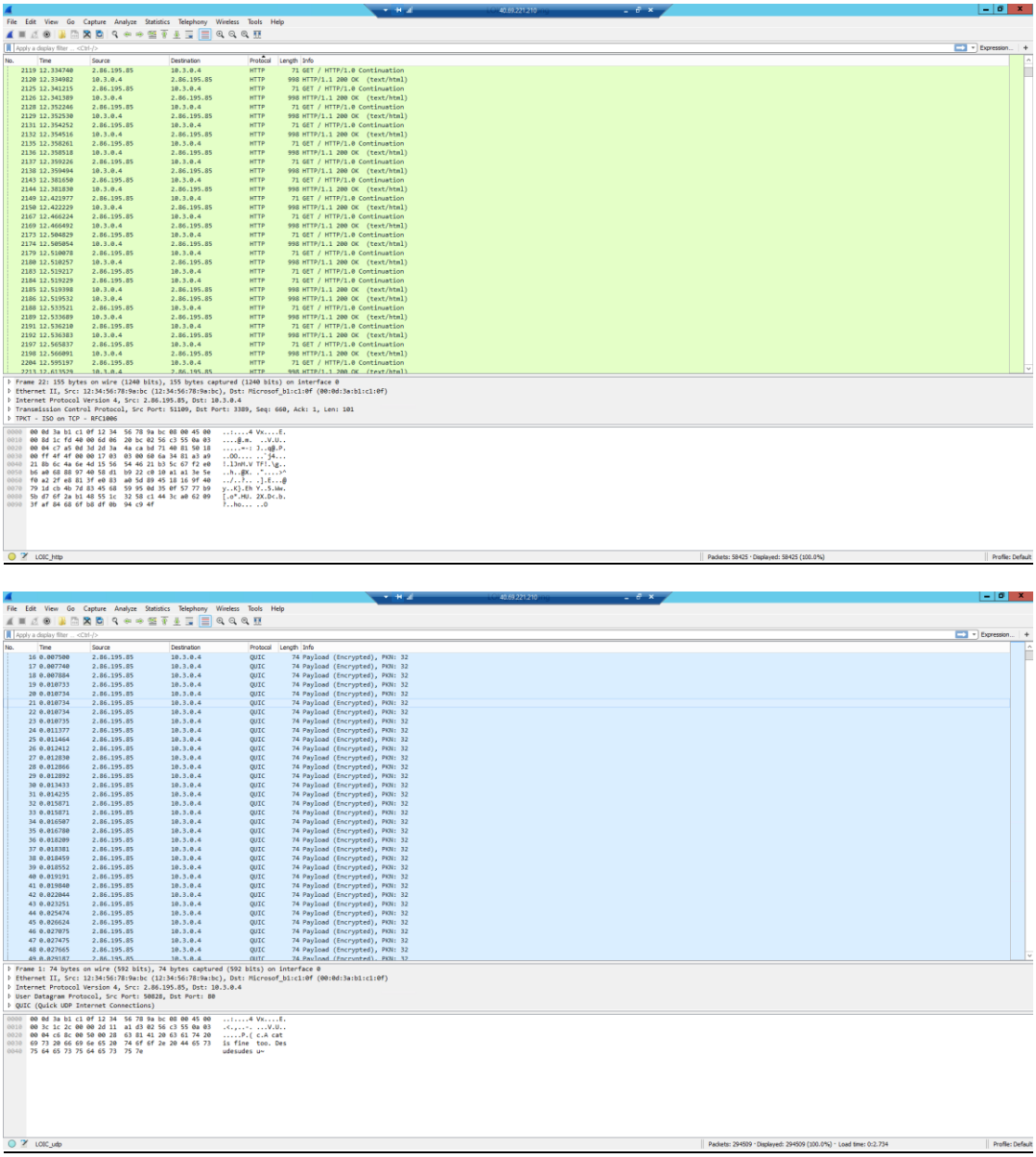
Επίθεση LOIC

Όλες οι παραπάνω επιθέσεις έγιναν μέσω λειτουργικού Kali-Linux, η επόμενη επίθεση θα εκτελεστεί μέσω Ubuntu-Linux, αποστέλλοντας http και udp πακέτα στον webserver.

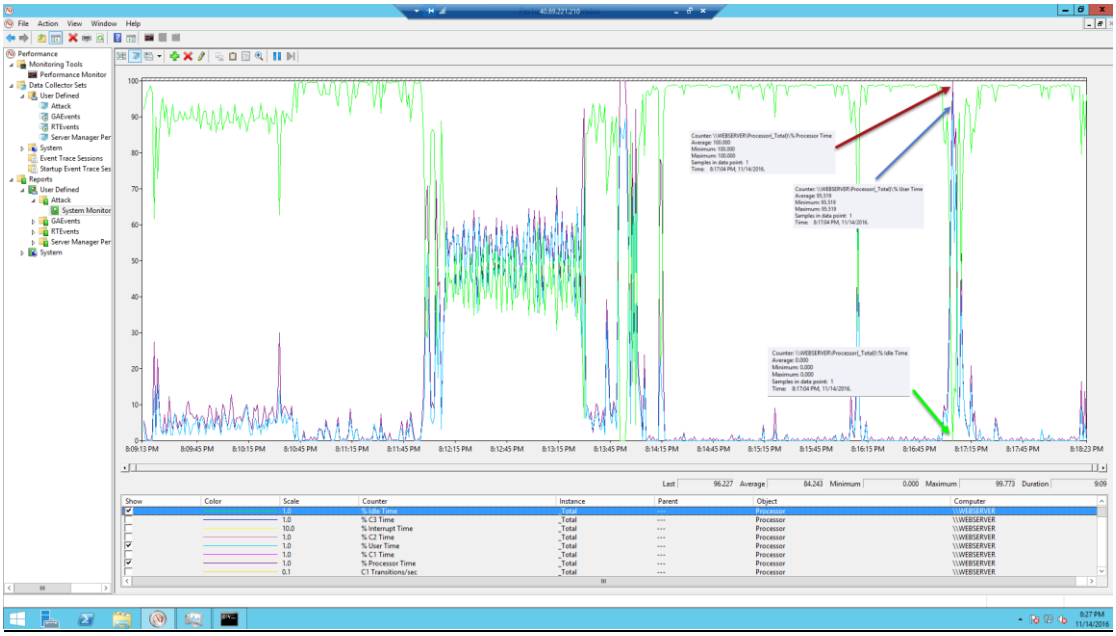


Εικόνα 4-49. LOIC Attack

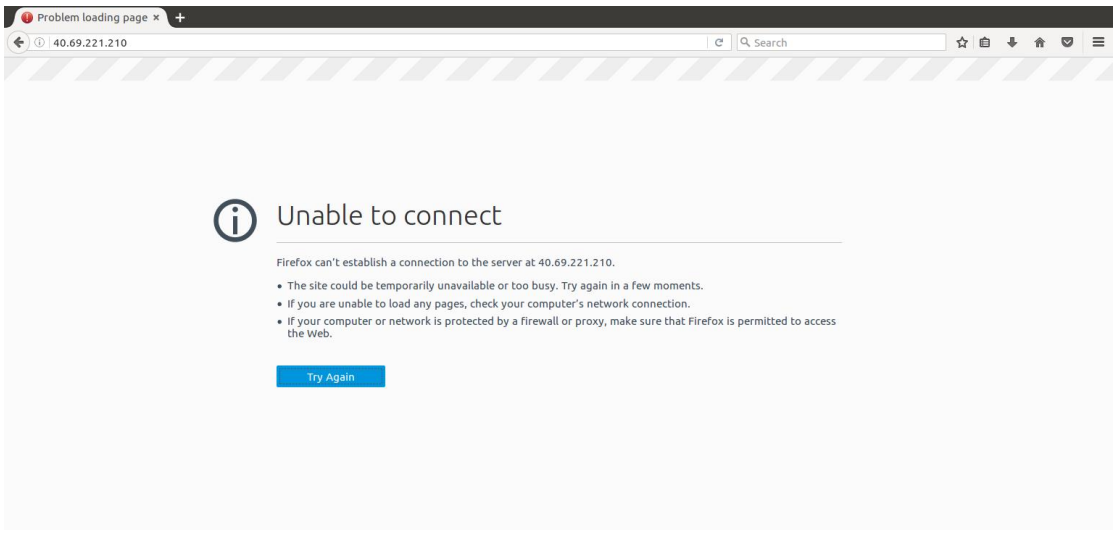
Με χρήση wireshark καταγράφονται τα http και udp (QUIC) πακέτα που προέρχονται από τον επιτιθέμενο και μέσω του “monitoring tool” των Windows φαίνεται η κατάσταση του συστήματος την στιγμή που η σελίδα γίνεται μη διαθέσιμη. Ο χρόνος που χρειάστηκε για να γίνει μη προσβάσιμη η σελίδα, με την επίθεση Loic ήταν πάνω από πέντε λεπτά.



Εικόνα 4-50. WireShark Capture



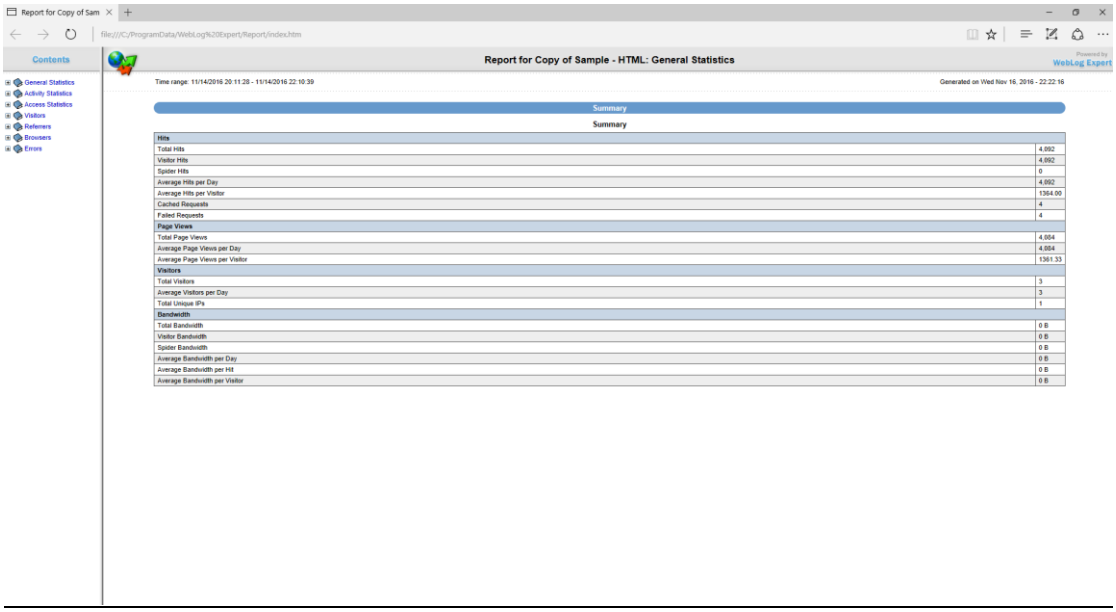
Εικόνα 4-51. Usage

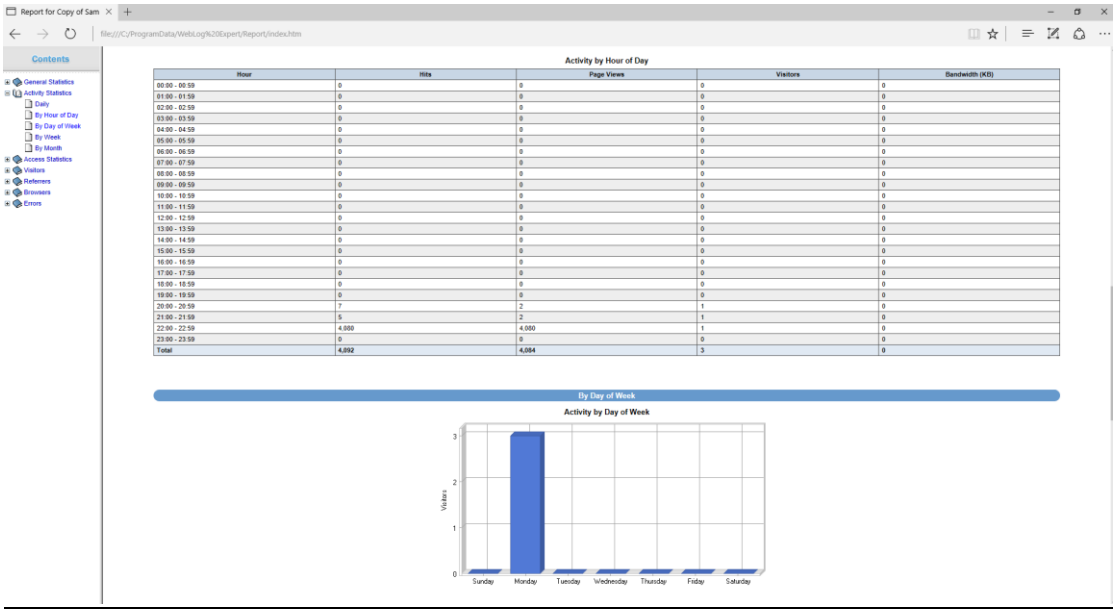


Εικόνα 4-52. Site Unavailability

Ανάλυση του log αρχείου του συστήματος

Με τη χρήση του προγράμματος WebLog expert αναλύουμε το log αρχείο του IIS το οποίο μας εμφανίζει τα “requests” που έγιναν, από τι είδους “browser” αλλά και λειτουργικό.

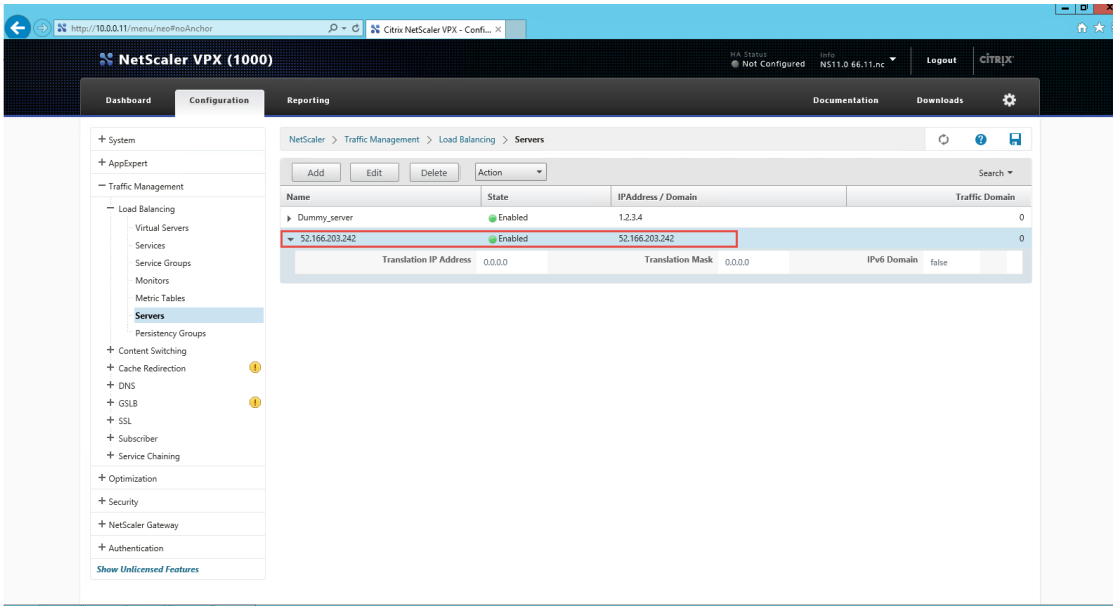

Report for Copy of Sam
Contents
General Statistics
Activity Statistics
Access Statistics
Visitors
Referrers
Browsers
Errors
Report for Copy of Sample - HTML: General Statistics
Powered by WebLog Expert
Time range: 11/14/2016 20:11:28 - 11/14/2016 22:10:39
Generated on Wed Nov 16, 2016 - 22:22:16
Summary
Summary
Hits
Total Hits 4,092
Visitor Hits 4,092
Spider Hits 0
Average Hits per Day 4,092
Average Hits per Visitor 1364.00
Cached Requests 4
Failed Requests 4
Page Views
Total Page Views 4,084
Average Page Views per Day 4,084
Average Page Views per Visitor 1361.33
Visitors
Total Visitors 3
Average Visitors per Day 3
Total Unique IPs 1
Bandwidth
Total Bandwidth 0 B
Visitor Bandwidth 0 B
Spider Bandwidth 0 B
Average Bandwidth per Day 0 B
Average Bandwidth per Hit 0 B
Average Bandwidth per Visitor 0 B


Report for Copy of Sam
Contents
General Statistics
Activity Statistics
Daily
By Hour of Day
By Day of Week
By Week
By Month
Access Statistics
Visitors
Referrers
Browsers
Errors
Activity by Hour of Day
Hour | Hits | Page Views | Visitors | Bandwidth (KB)
00:00 - 00:59 | 0 | 0 | 0 | 0
01:00 - 01:59 | 0 | 0 | 0 | 0
02:00 - 02:59 | 0 | 0 | 0 | 0
03:00 - 03:59 | 0 | 0 | 0 | 0
04:00 - 04:59 | 0 | 0 | 0 | 0
05:00 - 05:59 | 0 | 0 | 0 | 0
06:00 - 06:59 | 0 | 0 | 0 | 0
07:00 - 07:59 | 0 | 0 | 0 | 0
08:00 - 08:59 | 0 | 0 | 0 | 0
09:00 - 09:59 | 0 | 0 | 0 | 0
10:00 - 10:59 | 0 | 0 | 0 | 0
11:00 - 11:59 | 0 | 0 | 0 | 0
12:00 - 12:59 | 0 | 0 | 0 | 0
13:00 - 13:59 | 0 | 0 | 0 | 0
14:00 - 14:59 | 0 | 0 | 0 | 0
15:00 - 15:59 | 0 | 0 | 0 | 0
16:00 - 16:59 | 0 | 0 | 0 | 0
17:00 - 17:59 | 0 | 0 | 0 | 0
18:00 - 18:59 | 0 | 0 | 0 | 0
19:00 - 19:59 | 0 | 0 | 0 | 0
20:00 - 20:59 | 7 | 2 | 1 | 0
21:00 - 21:59 | 5 | 2 | 1 | 0
22:00 - 22:59 | 4,080 | 4,080 | 1 | 0
23:00 - 23:59 | 0 | 0 | 0 | 0
Total | 4,092 | 4,084 | 3 | 0
By Day of Week
Activity by Day of Week
Visitors
0
1
2
3
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Εικόνα 4-53. WebLog Expert Analysis

4.3.3 Επιθέσεις DDoS με στόχο την public IP του Netscaler

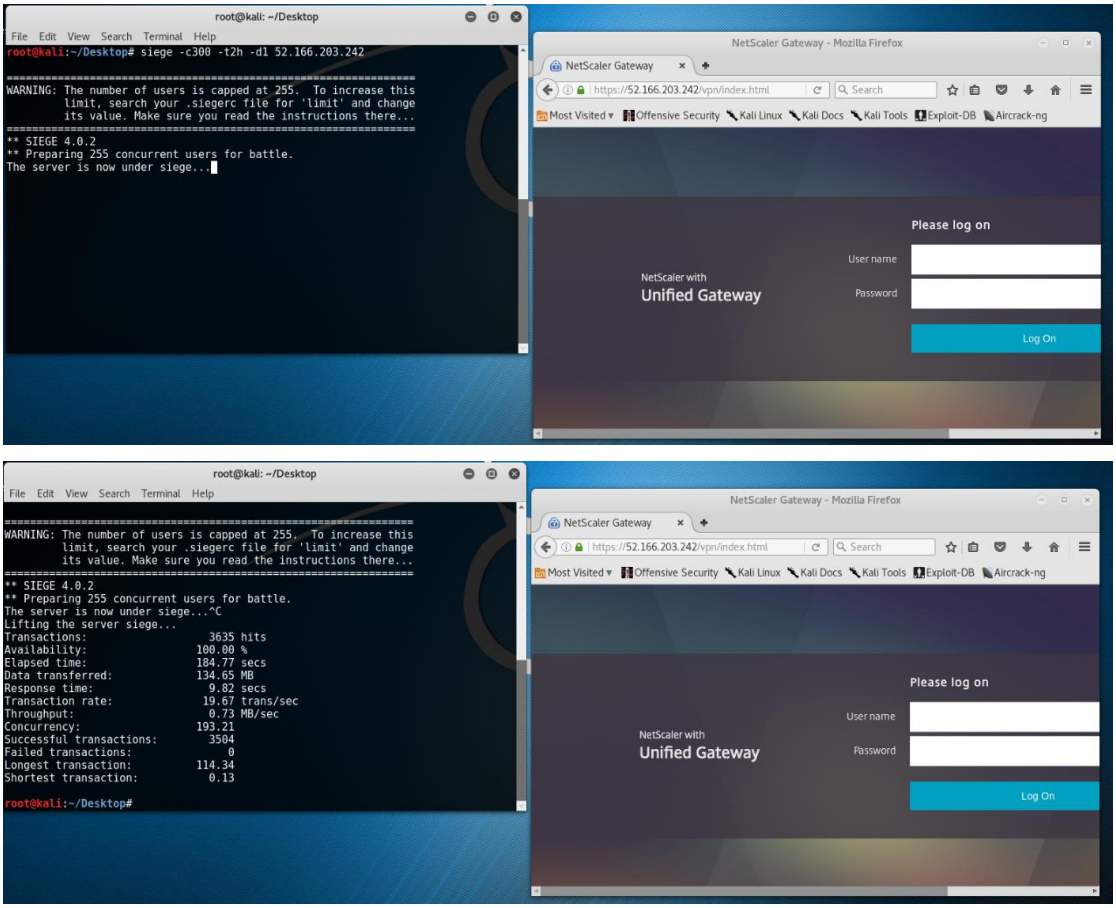
Όλες οι παραπάνω επιθέσεις ήταν επιτυχείς και κατέστησαν μη διαθέσιμες τις σελίδες, τόσο στον apache webserver όσο και στον IIS, προσβάλλοντας τα λειτουργικά συστήματα Linux και Windows αντίστοιχα. Οι δύο επιθέσεις που έφεραν πιο άμεσα αποτελέσματα ήταν η Siege και Slowloris, για αυτόν τον λόγο θα εφαρμοστούν στην public IP του Netscaler για να δούμε τα αποτελέσματα που θα επιφέρουν.



Εικόνα 4-54. Netscaler's IP

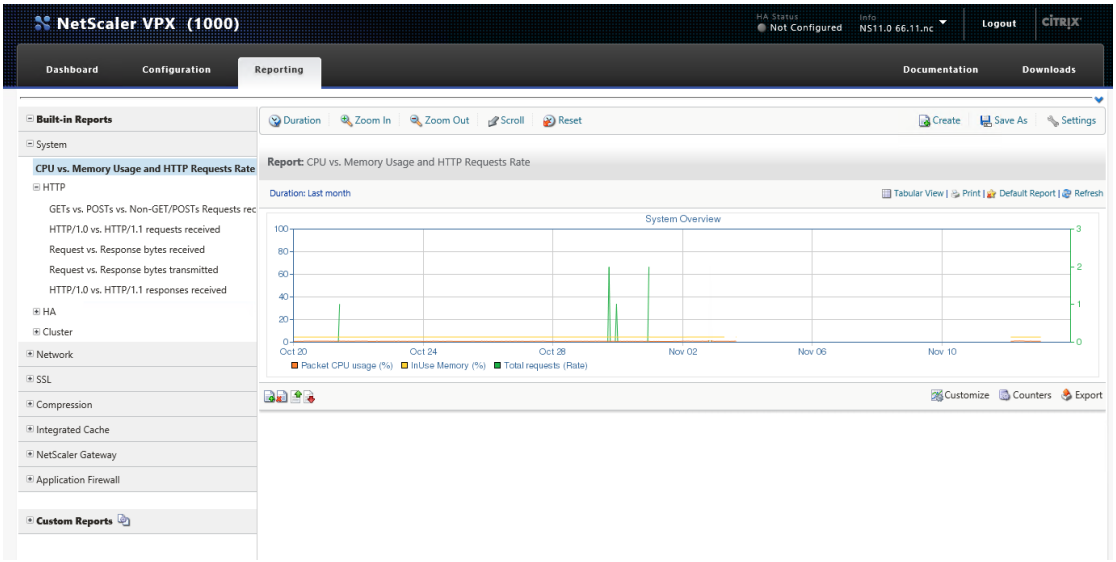
Τα αποτελέσματα που επέφεραν αυτές οι επιθέσεις φαίνονται παρακάτω, όπου διακρίνονται τα “requests” που έλαβε ο Netscaler. Η λήψη πολλών πακέτων – requests που έλαβε ο Netscaler βαθμολογούνται από τον ίδιο (Rate) ανάλογα με το πόσο ισχυρή ήταν η επίθεση και το πλήθος των requests. Αυτόν τον βαθμό θα χρησιμοποιήσουμε αργότερα για να δημιουργήσουμε έναν κανόνα με τον οποίο ο Netscaler θα απορρίπτει τα πακέτα όταν ο βαθμός-rate θα φτάνει στο σημείο που θα του ορίσουμε. Επίσης ένα πολύ σημαντικό σημείο το οποίο πρέπει να συνυπολογίσουμε είναι ότι, cpu και memory του συστήματος δεν επηρεάζονται καθόλου από τις επιθέσεις αυτές.

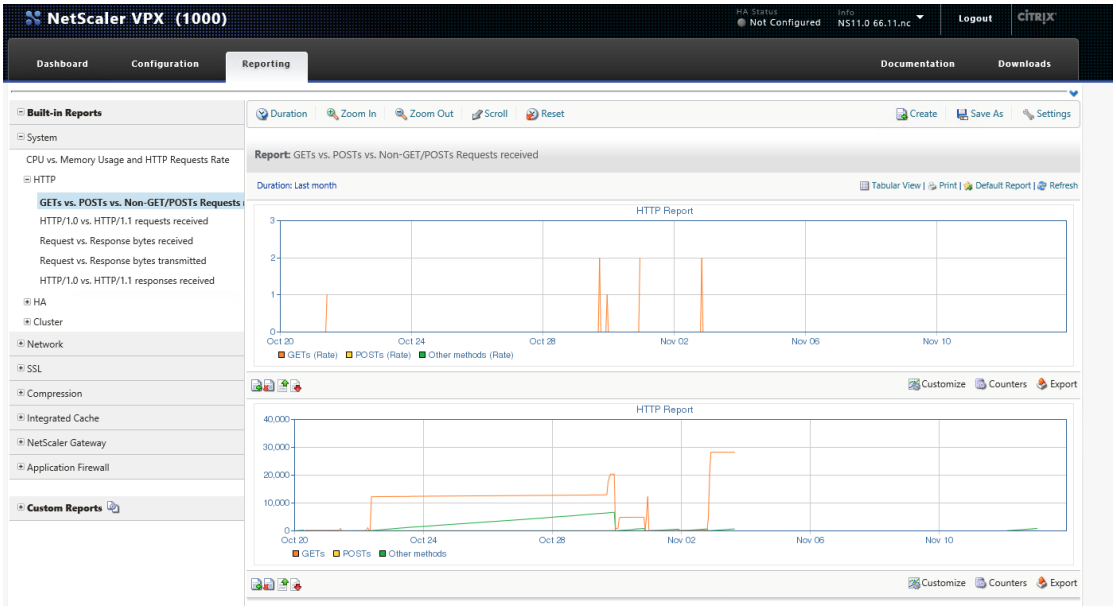
Επίθεση Siege

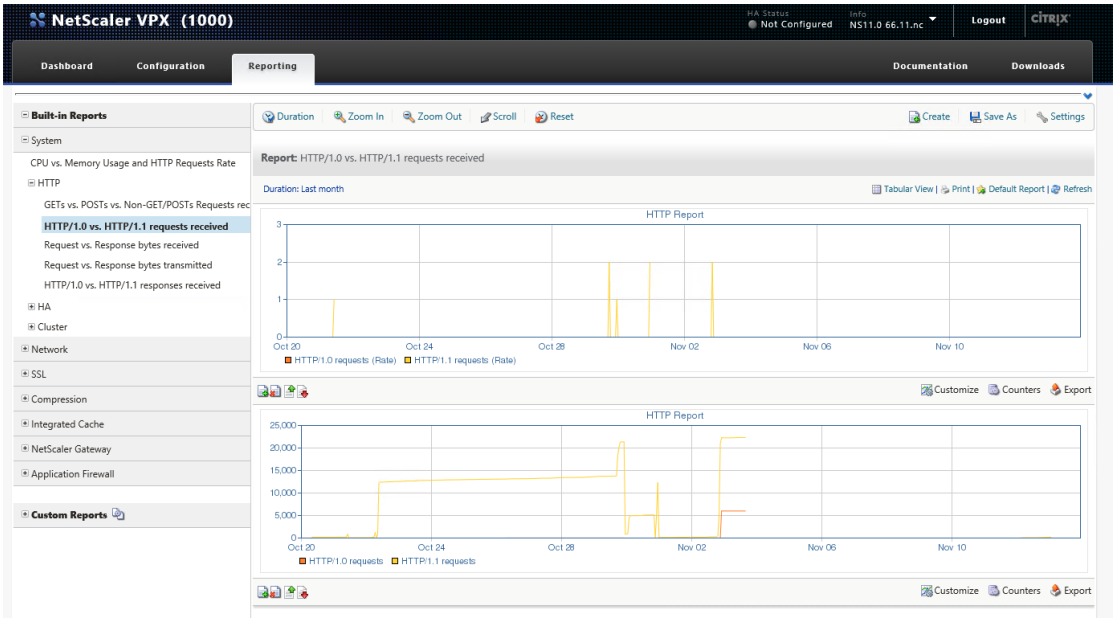


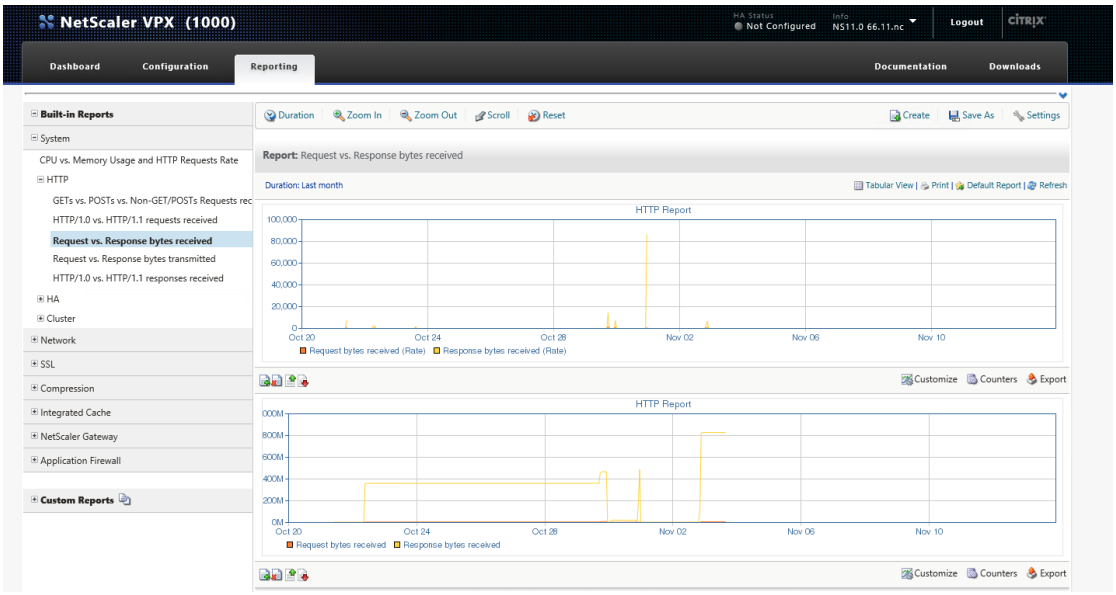
Εικόνα 4-55. Siege Attack

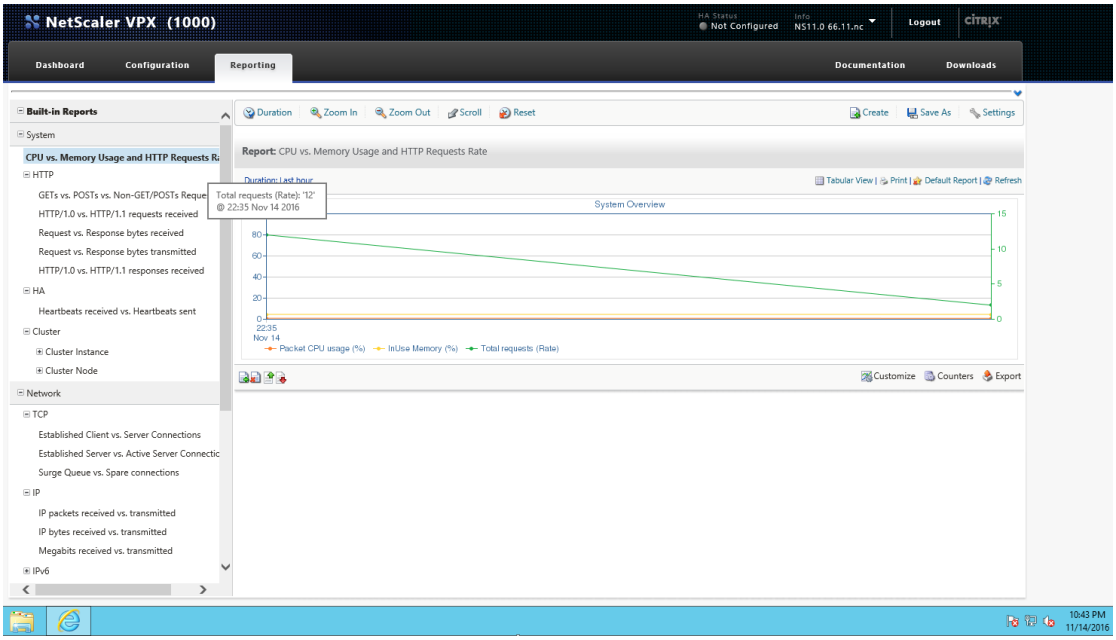
Αποτελέσματα:

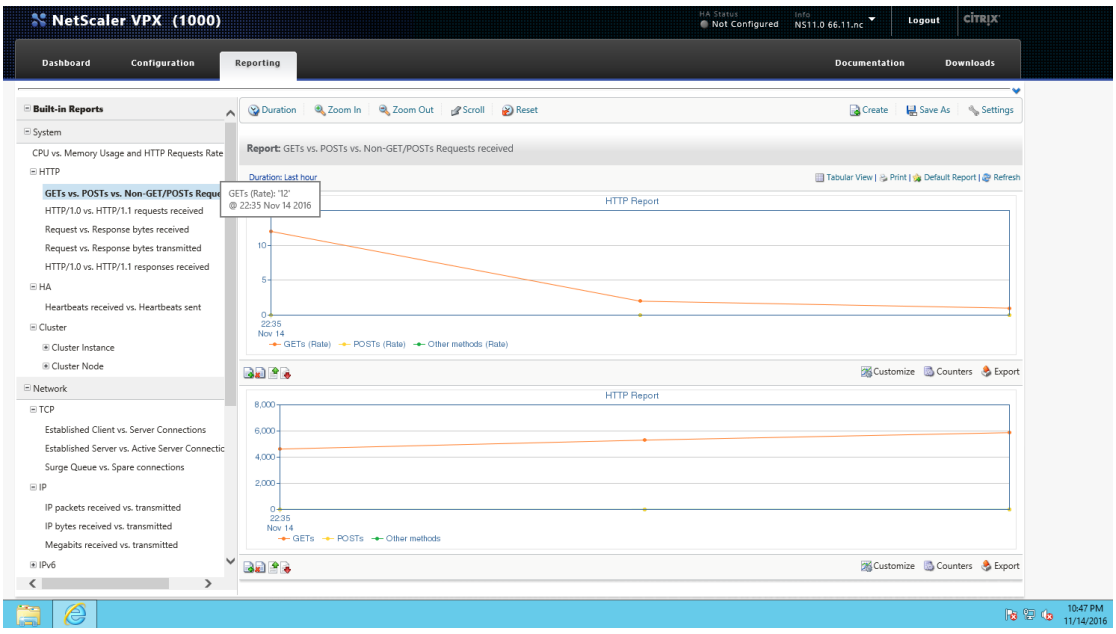


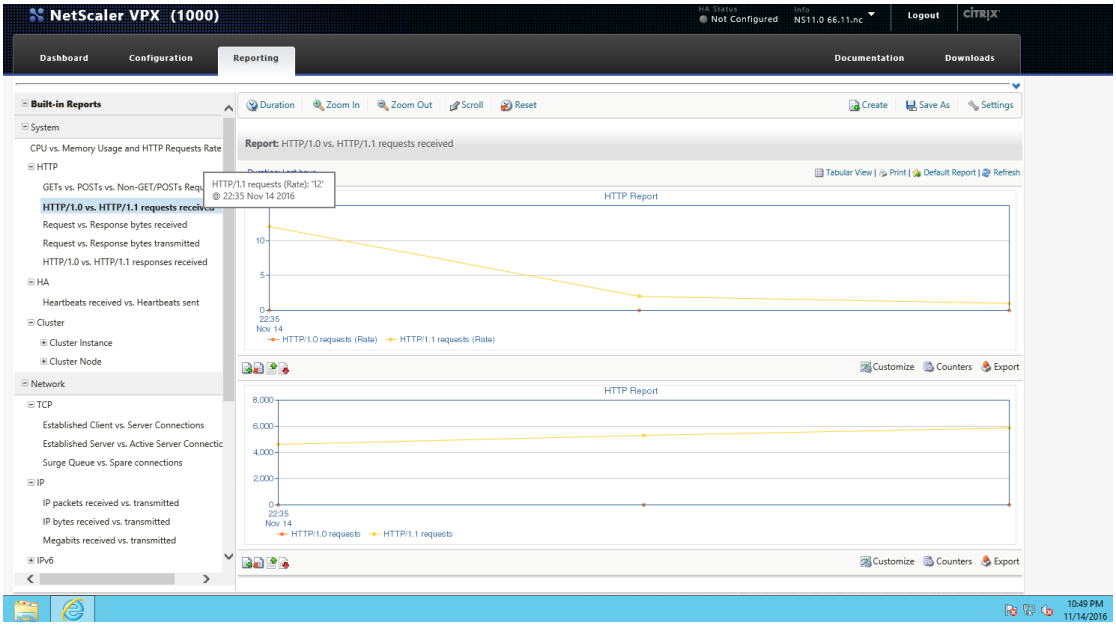

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Requests
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Cluster
Network
SSL
Compression
Integrated Cache
NetScaler Gateway
Application Firewall
Custom Reports
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: GETs vs. POSTs vs. Non-GET/POSTs Requests received
Duration: Last month
Tabular View | Print | Default Report | Refresh
HTTP Report
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Customize
Counters
Export
HTTP Report
GETs
POSTs
Other methods

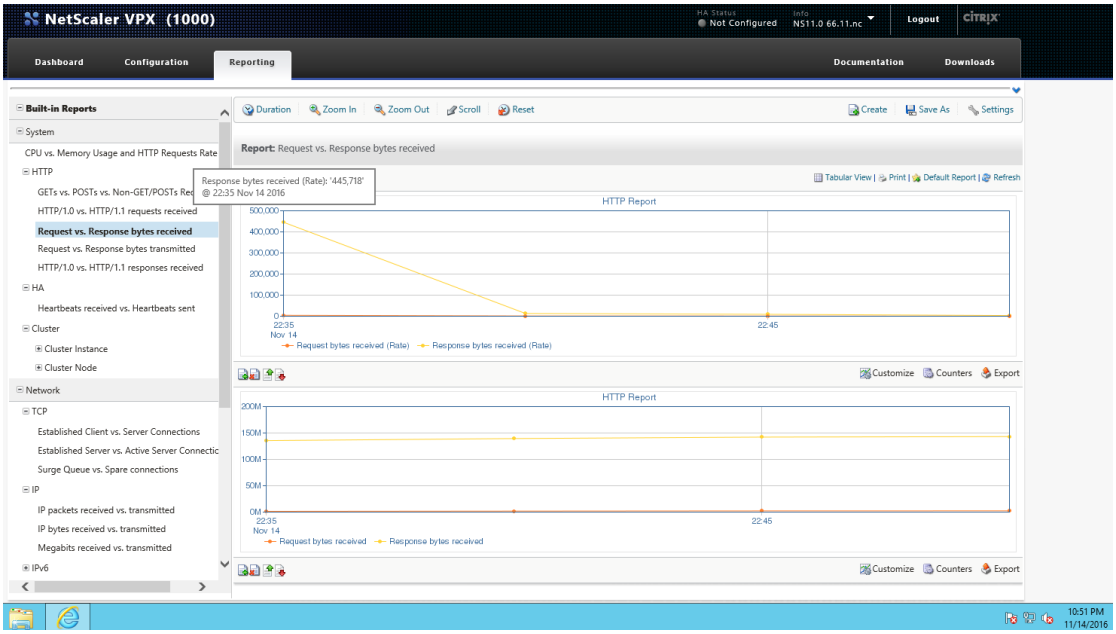

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Requests rec
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Cluster
Network
SSL
Compression
Integrated Cache
NetScaler Gateway
Application Firewall
Custom Reports
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: HTTP/1.0 vs. HTTP/1.1 requests received
Duration: Last month
Tabular View | Print | Default Report | Refresh
HTTP Report
HTTP/1.0 requests (Rate)
HTTP/1.1 requests (Rate)
Customize
Counters
Export
HTTP Report
HTTP/1.0 requests
HTTP/1.1 requests

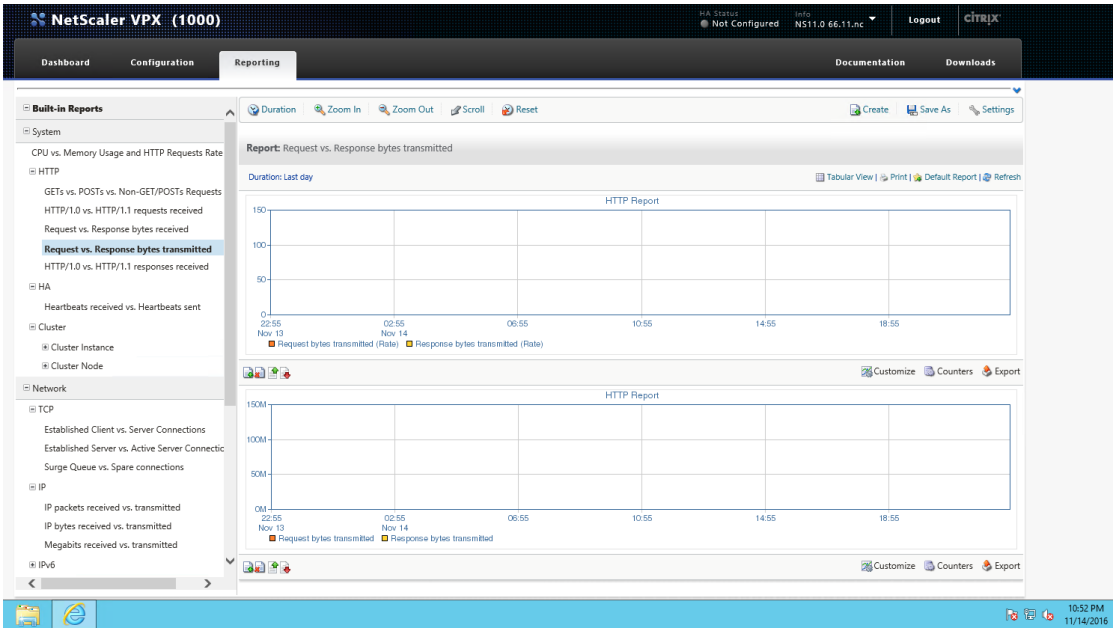

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Requests rec
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Cluster
Network
SSL
Compression
Integrated Cache
NetScaler Gateway
Application Firewall
Custom Reports
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: Request vs. Response bytes received
Duration: Last month
Tabular View | Print | Default Report | Refresh
HTTP Report
Request bytes received (Rate)
Response bytes received (Rate)
Customize
Counters
Export
HTTP Report
Request bytes received
Response bytes received

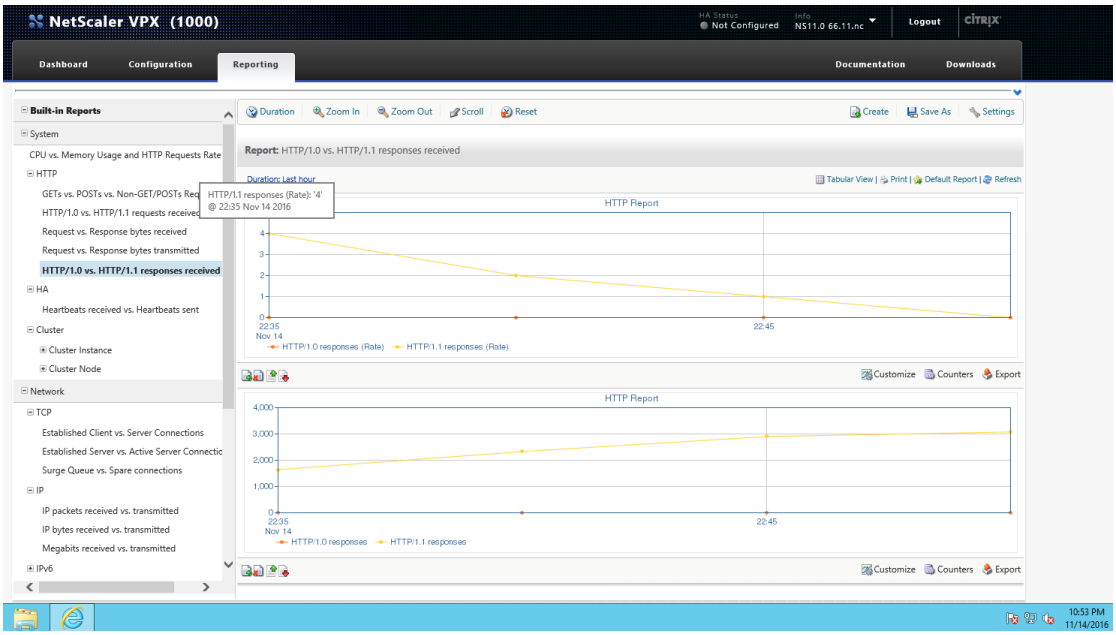

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests R
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Reque
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: CPU vs. Memory Usage and HTTP Requests Rate
Duration: Last hour
Tabular View | Print | Default Report | Refresh
Total requests (Rate): '12'
@ 22:35 Nov 14 2016
System Overview
Packet CPU usage (%)
InUse Memory (%)
Total requests (Rate)
Customize
Counters
Export
10:43 PM
11/14/2016

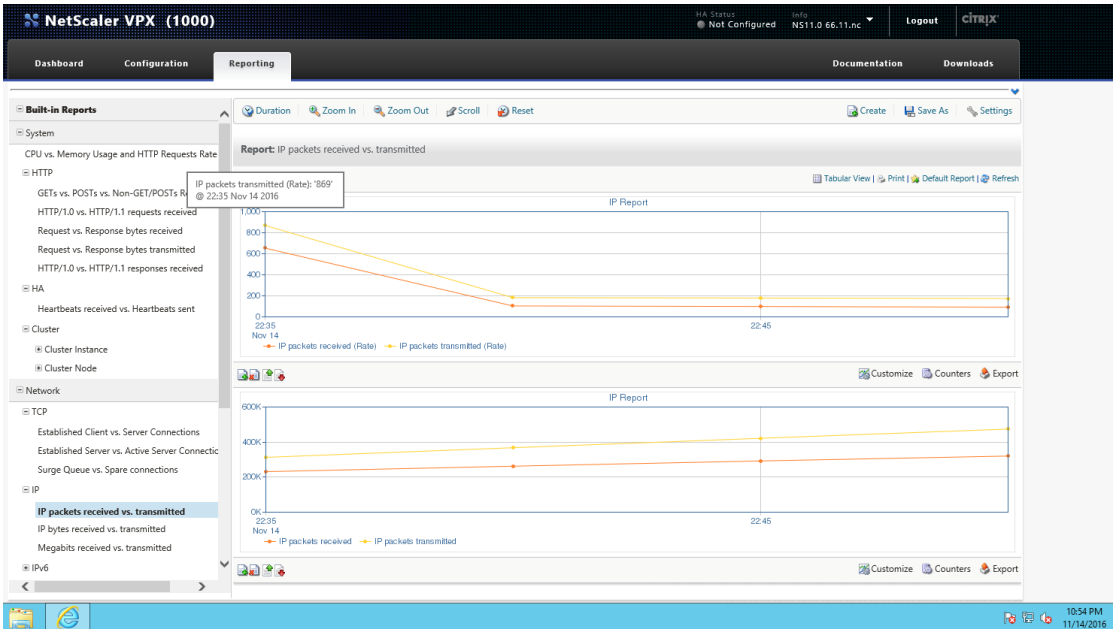

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Reque
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: GETs vs. POSTs vs. Non-GET/POSTs Requests received
Duration: Last hour
Tabular View | Print | Default Report | Refresh
GETs (Rate): '12'
@ 22:35 Nov 14 2016
HTTP Report
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Customize
Counters
Export
HTTP Report
GETs
POSTs
Other methods
Customize
Counters
Export
10:47 PM
11/14/2016

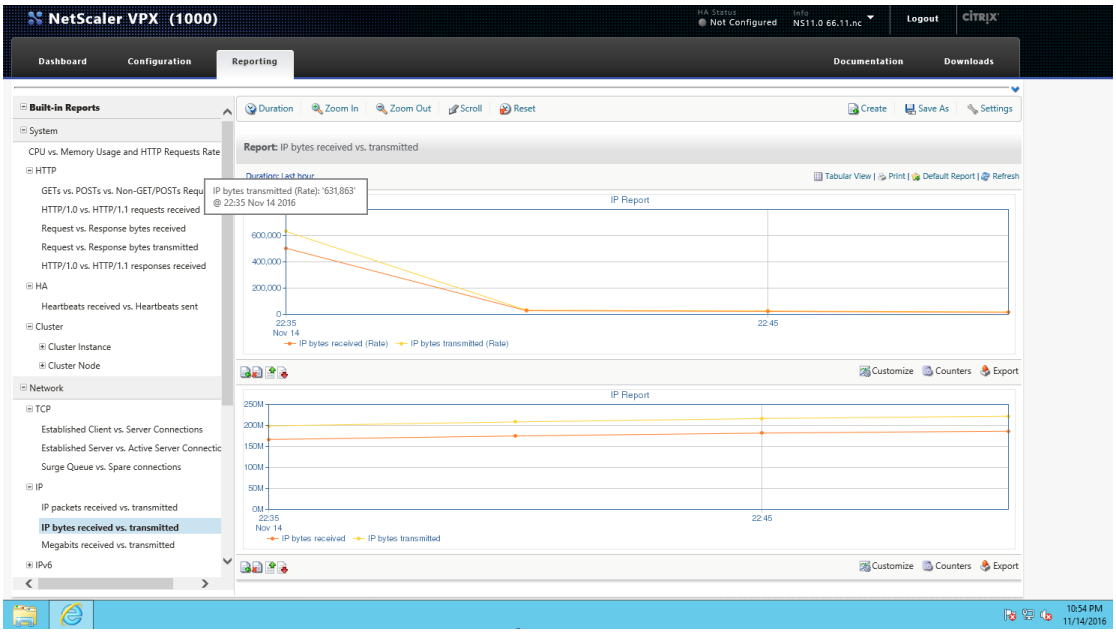

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Requ
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: HTTP/1.0 vs. HTTP/1.1 requests received
HTTP/1.1 requests (Rate): '12'
@ 22:35 Nov 14 2016
Tabular View | Print | Default Report | Refresh
HTTP Report
10
5
0
22:35
Nov 14
HTTP/1.0 requests (Rate)
HTTP/1.1 requests (Rate)
Customize
Counters
Export
HTTP Report
8,000
6,000
4,000
2,000
0
22:35
Nov 14
HTTP/1.0 requests
HTTP/1.1 requests
Customize
Counters
Export
10:49 PM
11/14/2016

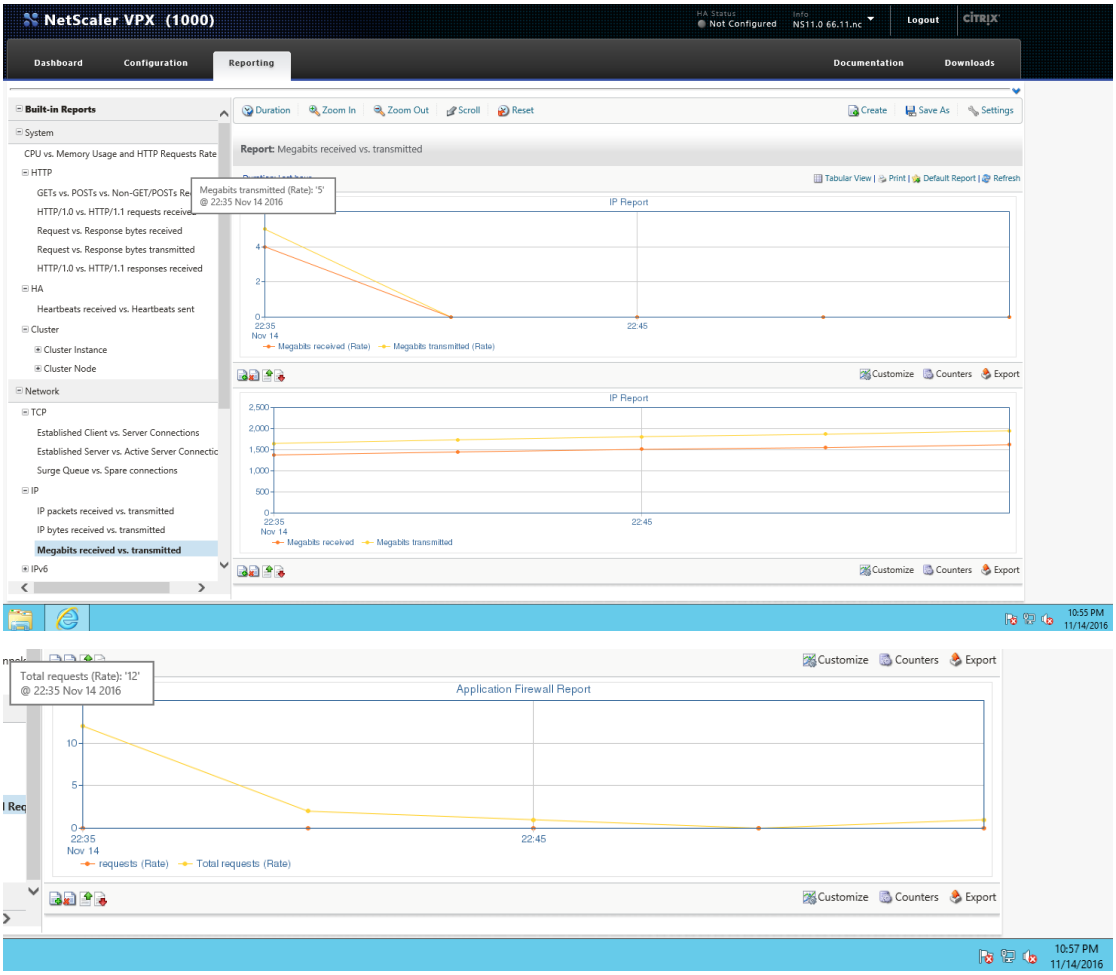

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Rec
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: Request vs. Response bytes received
Response bytes received (Rate): '445,718'
@ 22:35 Nov 14 2016
Tabular View | Print | Default Report | Refresh
HTTP Report
500,000
400,000
300,000
200,000
100,000
0
22:35
Nov 14
22:45
Request bytes received (Rate)
Response bytes received (Rate)
Customize
Counters
Export
HTTP Report
200M
150M
100M
50M
0M
22:35
Nov 14
22:45
Request bytes received
Response bytes received
Customize
Counters
Export
10:51 PM
11/14/2016


NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Requests
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: Request vs. Response bytes transmitted
Duration: Last day
Tabular View | Print | Default Report | Refresh
HTTP Report
150
100
50
0
22:55
Nov 13
02:55
Nov 14
06:55
10:55
14:55
18:55
Request bytes transmitted (Rate)
Response bytes transmitted (Rate)
Customize
Counters
Export
HTTP Report
150M
100M
50M
0M
Request bytes transmitted
Response bytes transmitted
10:52 PM
11/14/2016


NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Req
HTTP/1.0 vs. HTTP/1.1 requests receive
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
HTTP/1.1 responses (Rate): '4'
@ 22:35 Nov 14 2016
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: HTTP/1.0 vs. HTTP/1.1 responses received
Duration: Last hour
Tabular View | Print | Default Report | Refresh
HTTP Report
4
3
2
1
0
22:35
Nov 14
22:45
HTTP/1.0 responses (Rate)
HTTP/1.1 responses (Rate)
Customize
Counters
Export
HTTP Report
4,000
3,000
2,000
1,000
0
HTTP/1.0 responses
HTTP/1.1 responses
10:53 PM
11/14/2016

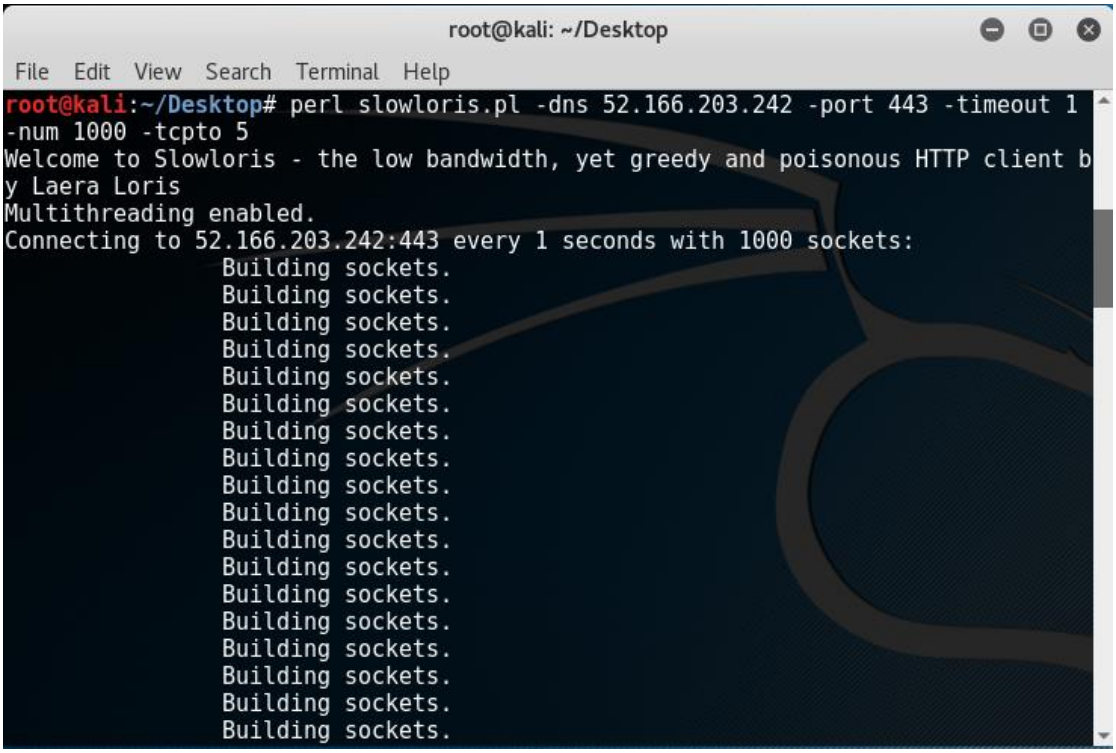

NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs R
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: IP packets received vs. transmitted
IP packets transmitted (Rate): '869'
@ 22:35 Nov 14 2016
Tabular View | Print | Default Report | Refresh
IP Report
1,000
800
600
400
200
0
22:35
Nov 14
22:45
IP packets received (Rate)
IP packets transmitted (Rate)
Customize
Counters
Export
IP Report
600K
400K
200K
0K
22:35
Nov 14
22:45
IP packets received
IP packets transmitted
Customize
Counters
Export
10:54 PM
11/14/2016


NetScaler VPX (1000)
HA Status
Not Configured
Info
NS11.0 66.11.nc
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Built-in Reports
System
CPU vs. Memory Usage and HTTP Requests Rate
HTTP
GETs vs. POSTs vs. Non-GET/POSTs Requ
HTTP/1.0 vs. HTTP/1.1 requests received
Request vs. Response bytes received
Request vs. Response bytes transmitted
HTTP/1.0 vs. HTTP/1.1 responses received
HA
Heartbeats received vs. Heartbeats sent
Cluster
Cluster Instance
Cluster Node
Network
TCP
Established Client vs. Server Connections
Established Server vs. Active Server Connectic
Surge Queue vs. Spare connections
IP
IP packets received vs. transmitted
IP bytes received vs. transmitted
Megabits received vs. transmitted
IPv6
Duration
Zoom In
Zoom Out
Scroll
Reset
Create
Save As
Settings
Report: IP bytes received vs. transmitted
Duration: Last hour
IP bytes transmitted (Rate): '631,863'
@ 22:35 Nov 14 2016
Tabular View | Print | Default Report | Refresh
IP Report
600,000
400,000
200,000
0
22:35
Nov 14
22:45
IP bytes received (Rate)
IP bytes transmitted (Rate)
Customize
Counters
Export
IP Report
250M
200M
150M
100M
50M
0M
22:35
Nov 14
22:45
IP bytes received
IP bytes transmitted
Customize
Counters
Export
10:54 PM
11/14/2016



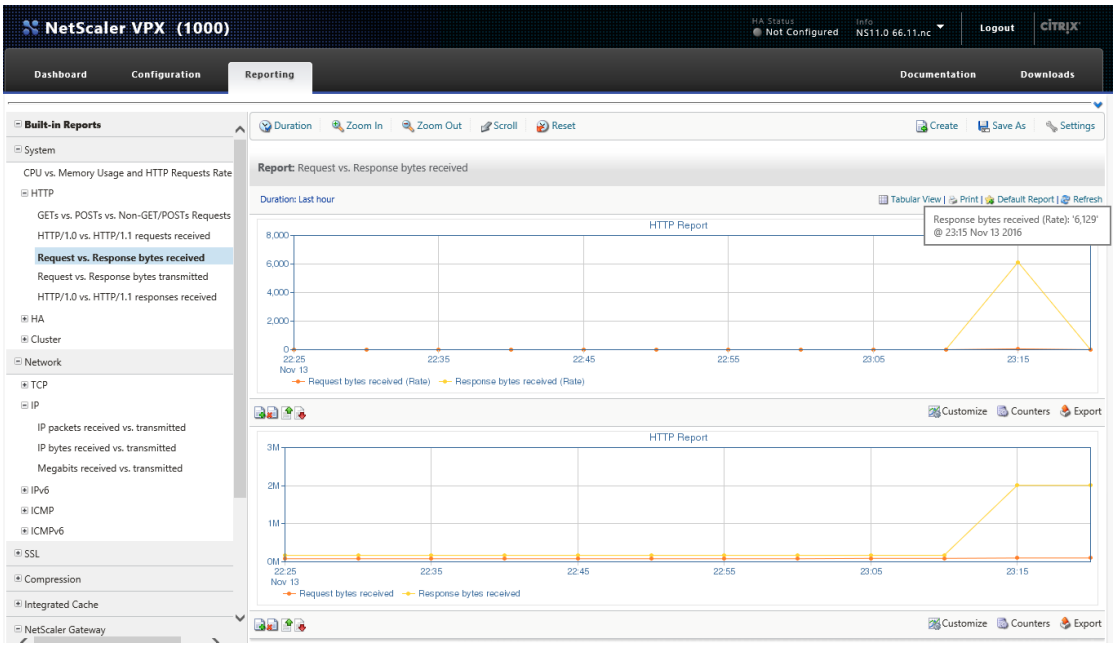
Εικόνα 4-56. Siege Results

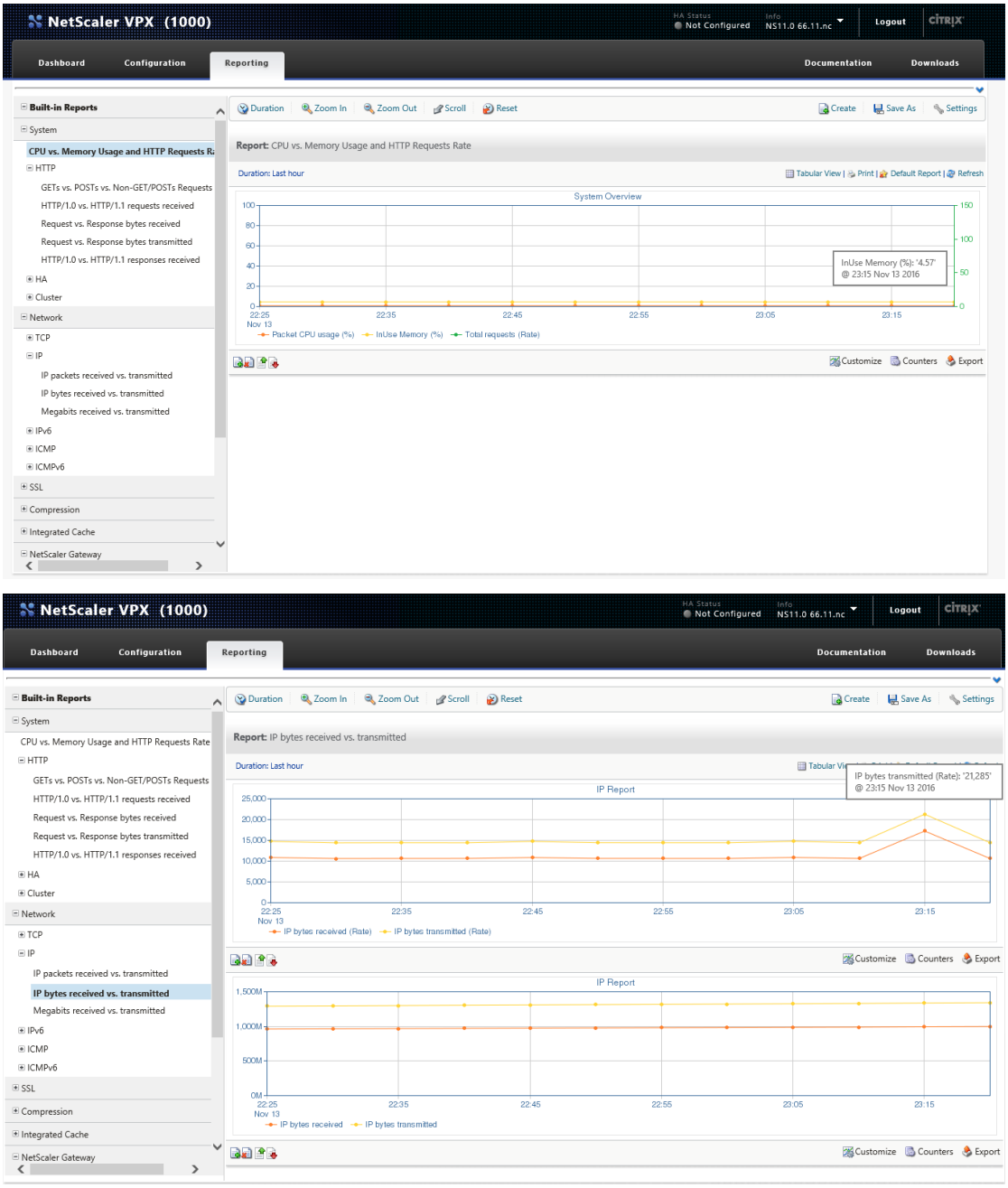
Επίθεση Slowloris



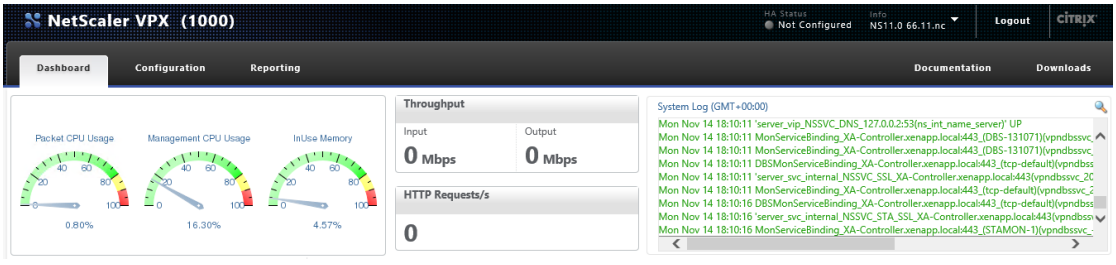
Εικόνα 4-57. Slowloris Attack

Αποτελέσματα:





Εικόνα 4-58. Slowloris Attack



Εικόνα 4-59. Netscaler's Usage

Όλες οι παραπάνω επιθέσεις εκτελέστηκαν στον Netscaler χωρίς να έχουν προστεθεί κανόνες αποφυγής DDoS επιθέσεων σε αυτόν όπως επίσης και οι ρυθμίσεις που

αναφέρθηκαν στην ενότητα 4.2.3 καθώς σε περίπτωση εφαρμογής των κανόνων ο Netscaler απορρίπτει τα πακέτα των επιτιθέμενων.

5 Συμπέρασμα

Ο Citrix Netscaler είναι μία συσκευή η οποία μπορεί να λειτουργήσει ως: *application delivery controller, load balancer* αλλά και *application firewall*, ενώ συγκαταλέγεται μέσα στις πέντε κορυφαίες λύσεις μαζί με τα παρακάτω προϊόντα,

- ✓ Barracuda 360
- ✓ F5 BIG-IP
- ✓ Dell SonicWall

Με την πάροδο των χρόνων ολοένα και περισσότερες εταιρείες χρησιμοποιούν τεχνολογίες cloud και αυτό καθιστά απαραίτητη την εγκατάσταση και χρήση τέτοιων συσκευών, οι οποίες με την κατάλληλη παραμετροποίηση μπορούν να συνεισφέρουν στην μείωση των κενών ασφαλείας μιας υποδομής.

Ας μην ξεχνάμε όμως ότι η ασφάλεια μιας υποδομής δεν μπορεί να περιοριστεί μόνο με τη χρήση μίας συσκευή καθώς είναι αποτέλεσμα συνολικών μέτρων, ξεκινώντας από την κατάλληλη εκπαίδευση των χρηστών και καταλήγοντας στην επιβολή μέτρων και κανόνων ασφαλείας σε κάθε επίπεδο της υποδομής και σε όλα τα μέρη από τα οποία αποτελείται αυτή.

Η πρόληψη, η συνεχής ενημέρωση και εκπαίδευση, η συμμόρφωση με τους κανόνες, η μεθοδευμένη εργασία, η κατανόηση της σημαντικότητας της ασφάλειας, είναι τα συστατικά εκείνα που μπορούν να οδηγήσουν στην αποτελεσματικότερη αντιμετώπιση των απειλών ασφαλείας που συνεχώς αυξάνονται.

Βιβλιογραφία

1. Jinesh Varia, Amazon Web Services "Architecting for The Cloud: Best Practices", January 2011
2. Qi Zhang, Lu Cheng, Raouf Boutaba "Cloud computing: state-of-the-art and research challenges", J Internet Serv Appl, April 2010
3. Staten James "Which Cloud Computing Platform is right for you?", Forrester Research Inc., April 2009
4. Enisa "Cloud Computing Benefits, risks and recommendations for information security", December 2012
5. Citrix Netscaler Getting Started Guide, May 2010
6. Citrix Netscaler Global Server Load Balancing Primer: Theory and Implementation
7. Dual Secure Ticket Authority Ticketing Architecture, March 2014
8. NetScaler for the best XenApp/XenDesktop access and mobile experience, whitepaper, citrix.com
9. NetScaler VPX, Data Sheet, citrix.com
10. Deliver applications as a cost effective, on-demand service to any user, anywhere, citrix.com
11. End-To-End Encryption with XenApp and XenDesktop, whitepaper, citrix.com
12. How to Configure NetScaler Gateway 10.5 to use with StoreFront 2.6 and XenDesktop 7.6., whitepaper, citrix.com

13. https://www.ibm.com/developerworks/community/blogs
14. http://www.cmswire.com/cms/information-management/cloud-service-models
15. http://www.logicworks.net/blog/
16. https://en.wikipedia.org/wiki/Cloud_computing
17. http://www.intel.com/content/video
18. http://docs.Citrix.com/
19. https://blogs.msdn.microsoft.com/
20. https://www.blackmoreops.com/
21. https://www.wireshark.org/
22. http://askubuntu.com/
23. https://www.kali.org/
24. https://www.ubuntu.com/