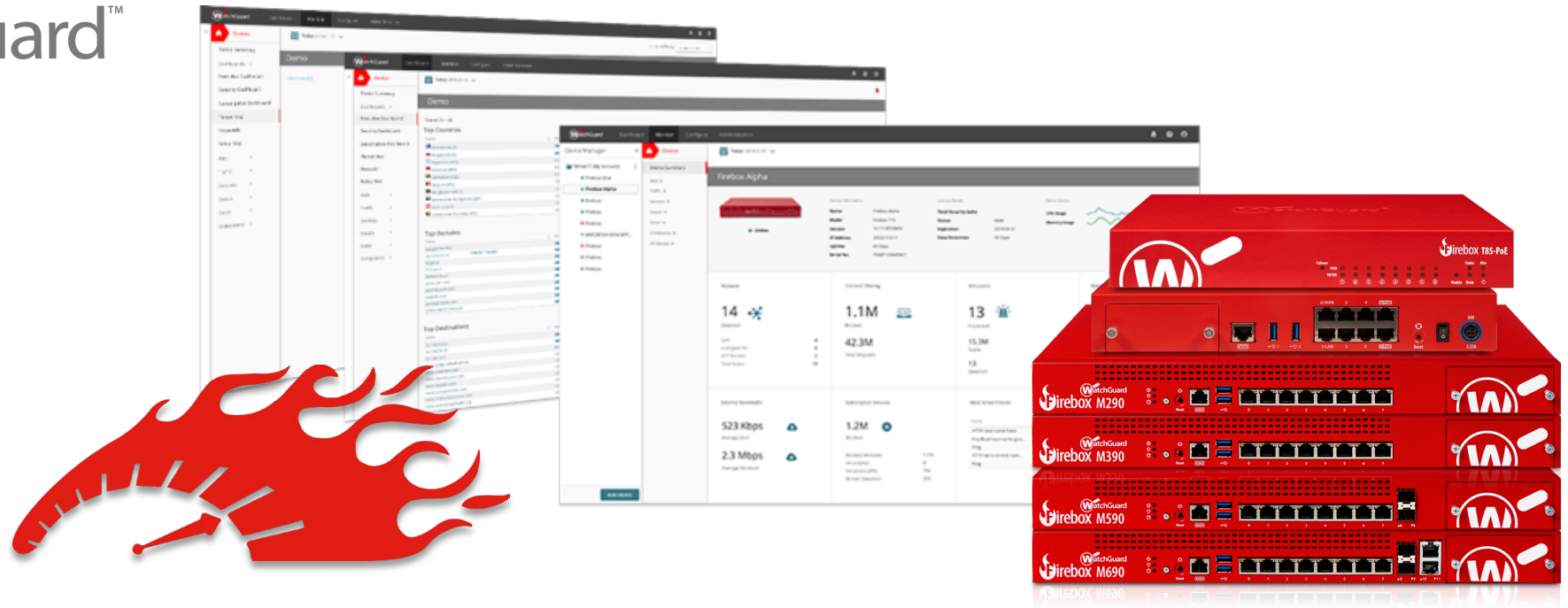
Ο ρόλος του Firewall στο Penetration Test.

Εισήγηση:
Αντώνης Καλοχριστιανάκης, Διευθυντής Πωλήσεων | Digital SIMA
Γιάννης Δασκαλόπουλος, Security Services Supervisor | Digital SIMA

WatchGuard™



Ενιαία cloud πλατφόρμα διαχείρισης

Βήματα ενίσχυσης της Κυβερνοασφάλειας

- Ενσωμάτωση μηχανισμών και διαδικασιών ασφάλειας του δικτύου.
- Έλεγχοι ασφάλειας (Pen-Test, Audit κ.λ.π).
- Αποκατάσταση ευπαθειών.
- User Awareness.
- Επανέλεγχοι.

Ποιοι κάνουν Security Services

- Εταιρείες που πραγματικά θέλουν να θωρακίσουν το δίκτυο και να ανιχνεύσουν κινδύνους.
- Εταιρείες που υποχρεώνονται από τα κανονιστικά πλαίσια του κλάδου τους.
- Εταιρείες που τους απαιτείται από άλλες εταιρίες ως προϋπόθεση συνεργασίας.
- Εταιρείες που θέλουν να συμμετάσχουν σε έργα (διαγωνισμοί κ.λ.π.) που απαιτείται ως προϋπόθεση συμμετοχής.
- Εταιρείες που θέλουν να μεγαλώσουν την αξία τους και να βελτιώσουν το προφίλ τους.

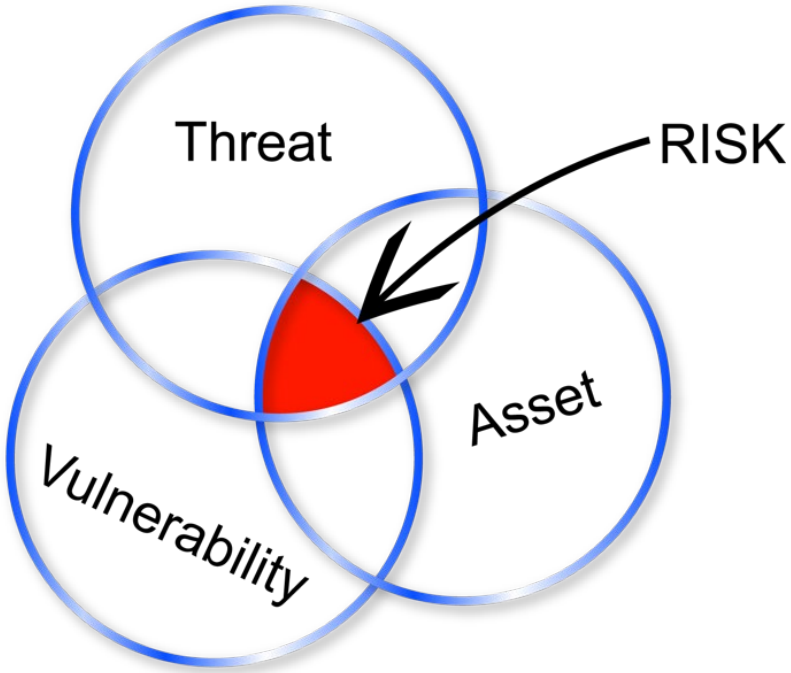
Penetration Test

Έλεγχος κρίσιμων στοιχείων
(Firewall, Active Directory, Email Server, SQL Server και Web Server)

- ✓ Αυτοματοποιημένα εργαλεία.
- ✓ Προσπάθεια παρείσδυσης από εξειδικευμένη ομάδα τεχνικών.
- ✓ Έλεγχος για γνωστές αλλά και άγνωστες ευπάθειες όπως λάθη, παραλείψεις ή πρόβλημα στο σχεδιασμό.

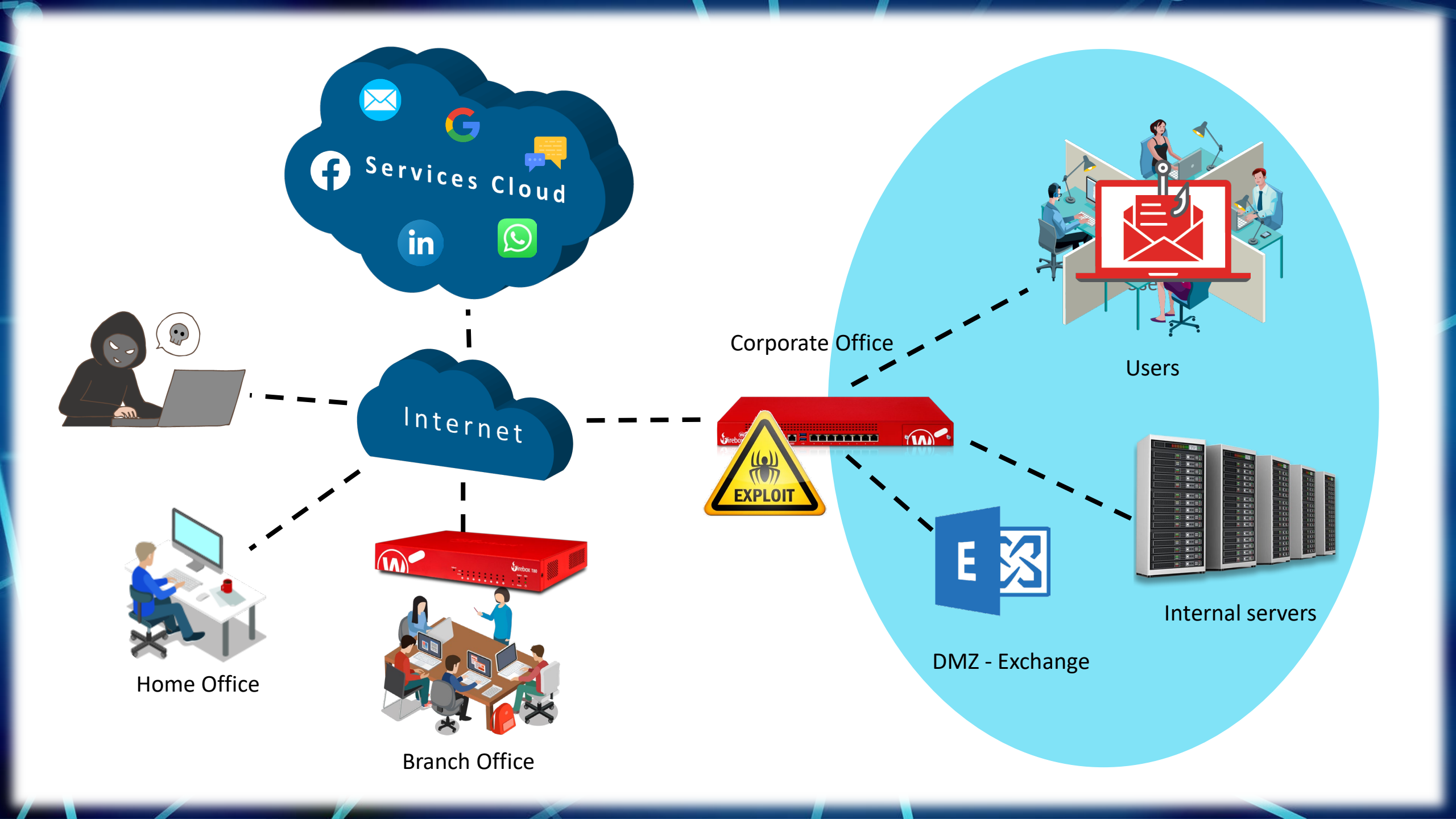
Αποτέλεσμα:

- Καταγραφή και αξιολόγηση των κινδύνων.
- Προτεινόμενες ενέργειες για την διόρθωσή τους.



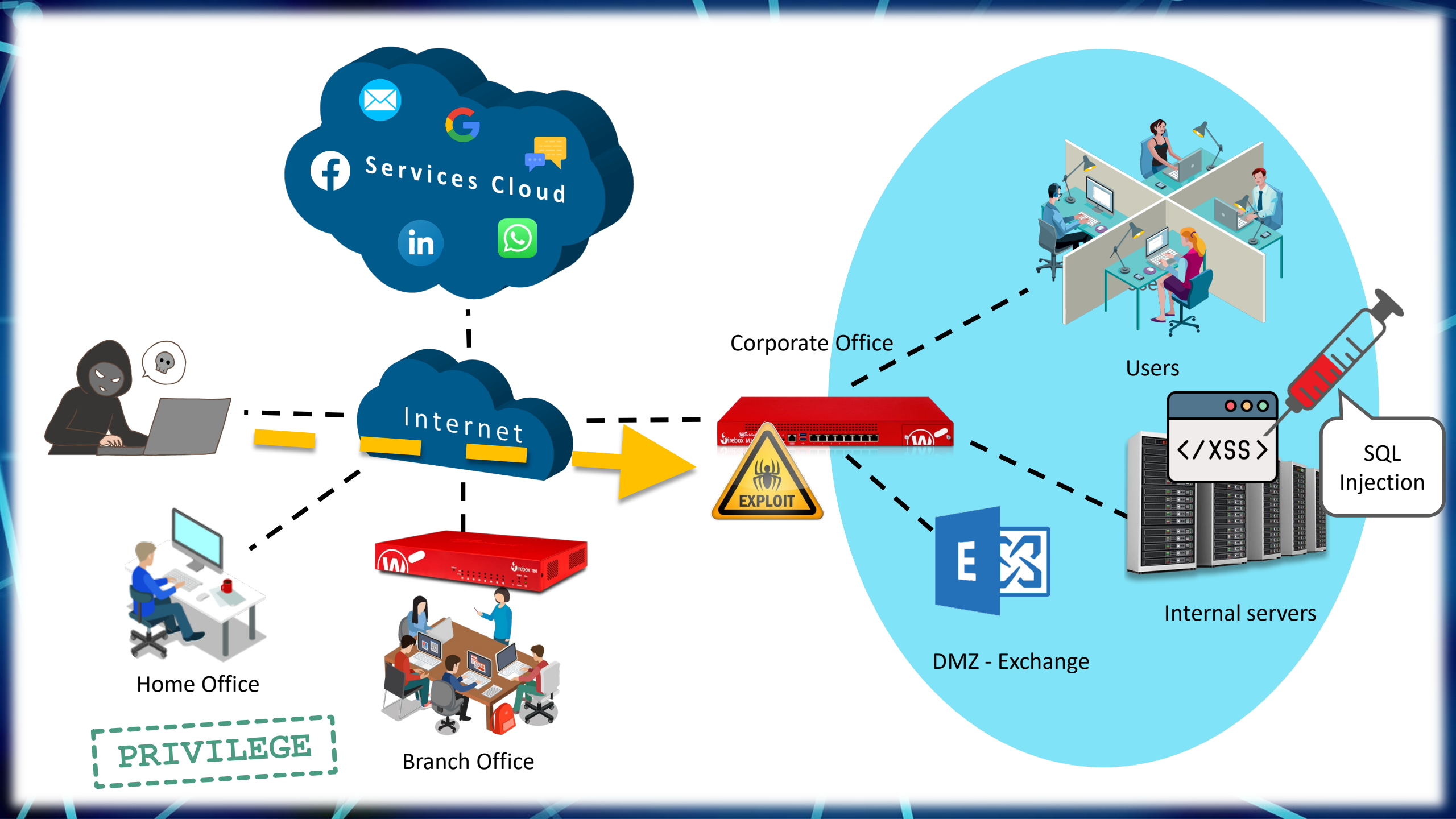
Penetration Test

Αν κάνω Internal γιατί να κάνω και External Penetration;


Services Cloud
Internet
Corporate Office
Users
EXPLOIT
Internal servers
DMZ - Exchange
Home Office
Branch Office

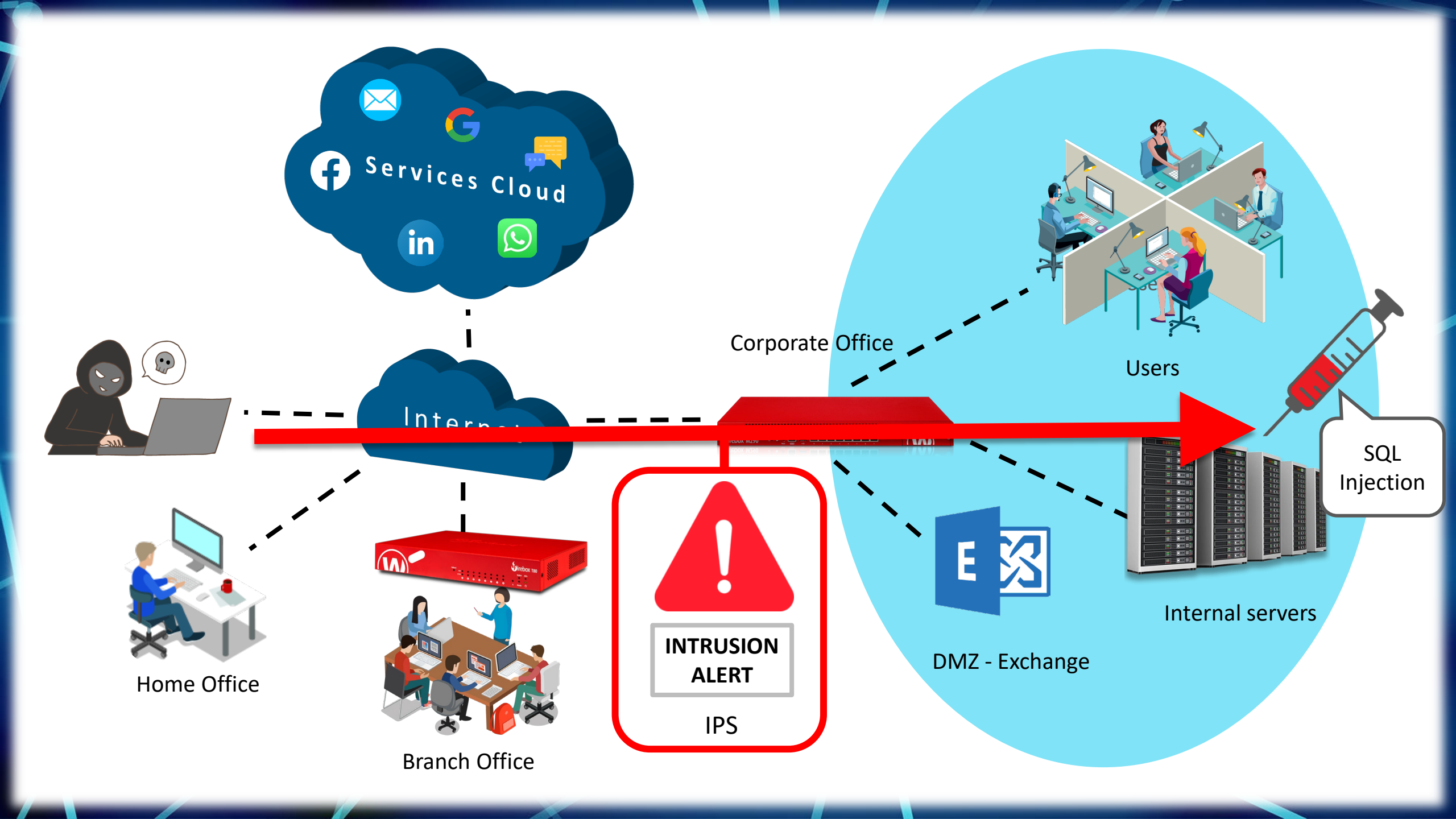
Penetration Test

Ποια προβλήματα του NG Firewall αναδεικνύονται;


Services Cloud
Internet
Corporate Office
Users
EXPLOIT
</XSS>
SQL Injection
Internal servers
DMZ - Exchange
Home Office
Branch Office
PRIVILEGE

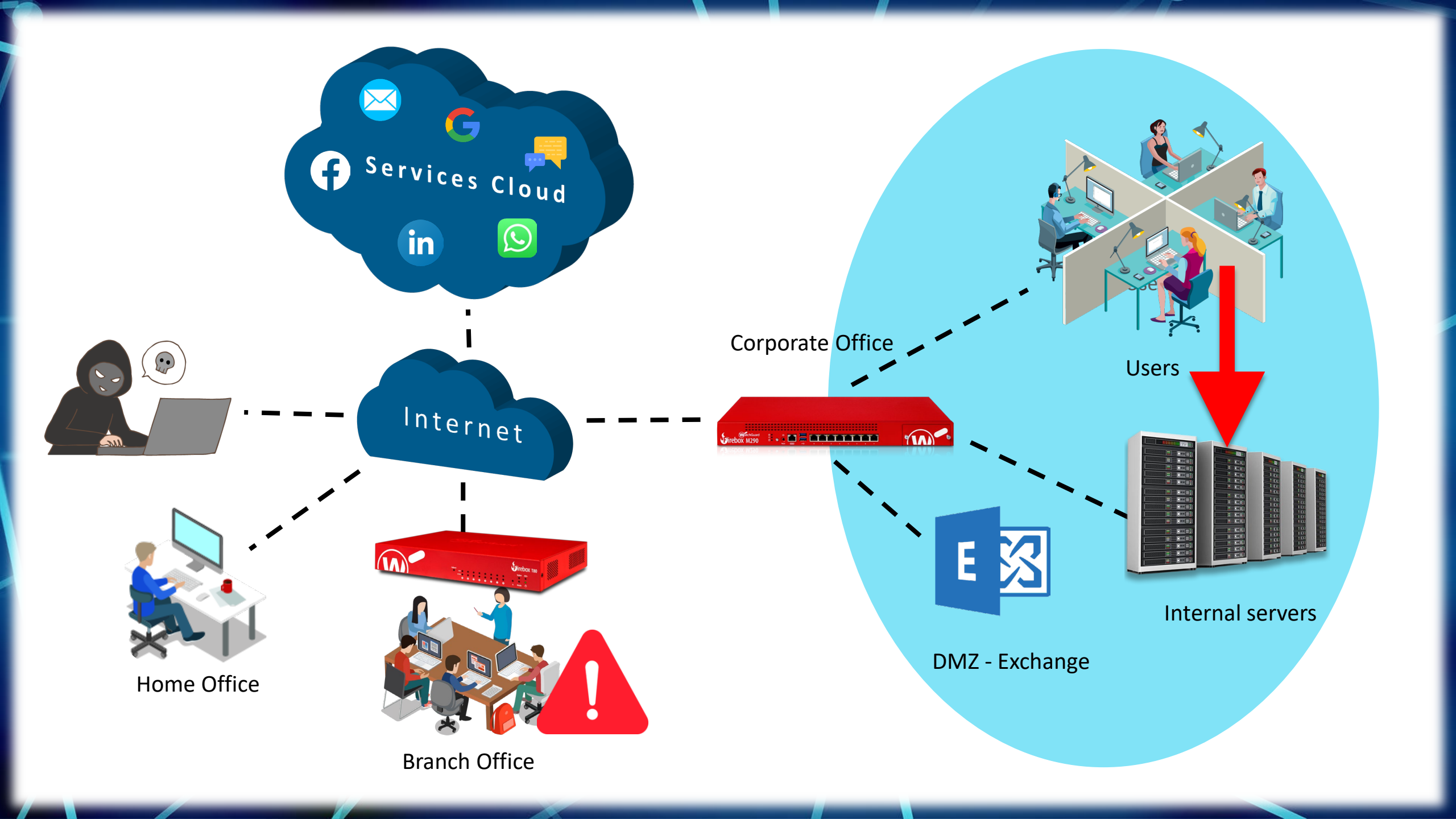
Penetration Test

Τι ευρήματα αποκρύπτονται από το NG Firewall;


Services Cloud
Internet
Corporate Office
Users
SQL Injection
Internal servers
DMZ - Exchange
INTRUSION ALERT
IPS
Home Office
Branch Office

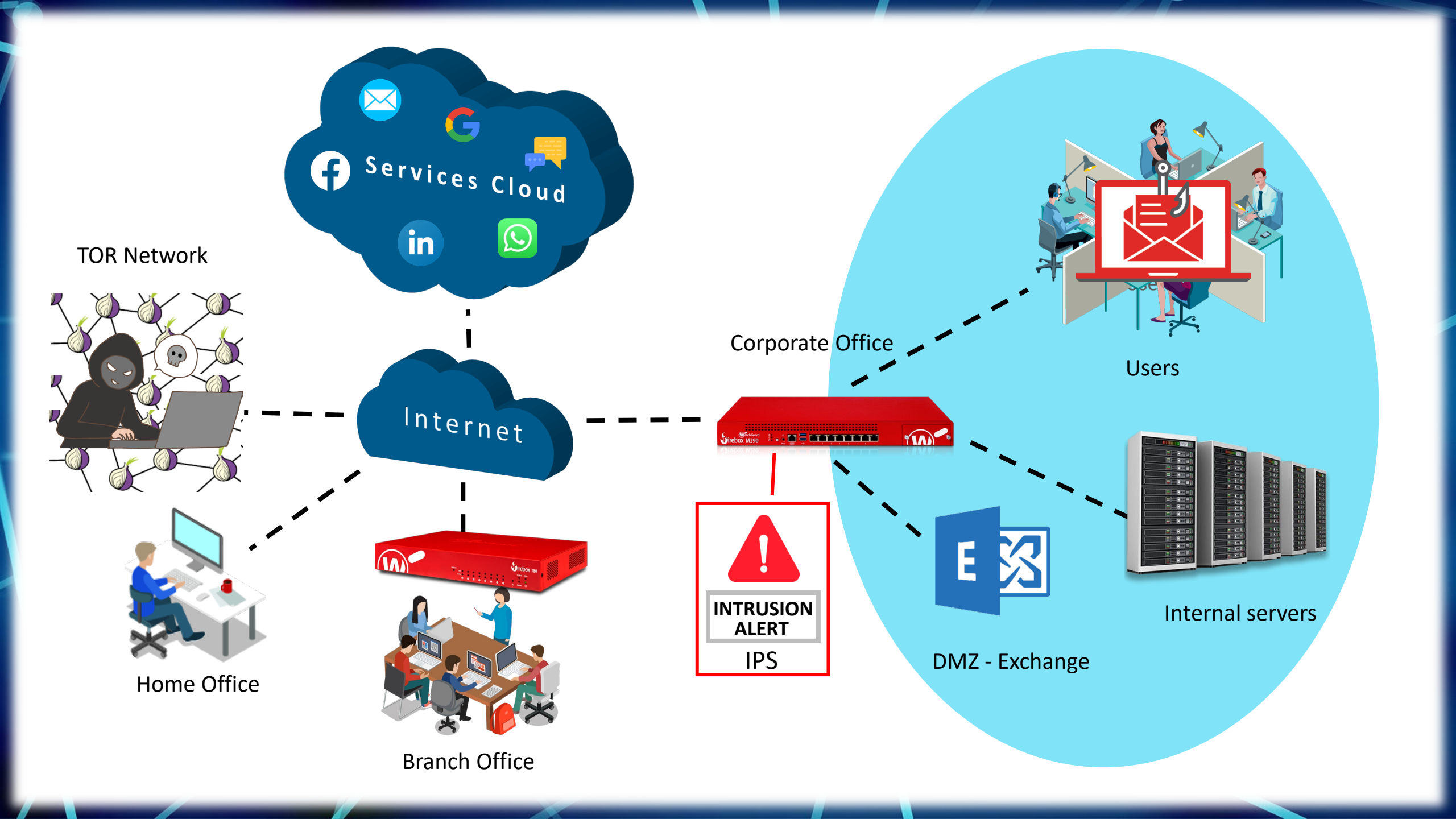
Penetration Test

Υπάρχουν διαφοροποιήσεις σε ένα Internal Penetration Test; (σενάρια, δικαιώματα)


Services Cloud
Internet
Corporate Office
Users
Internal servers
DMZ - Exchange
Home Office
Branch Office

Penetration Test

Υπάρχουν διαφοροποιήσεις σε ένα External Penetration Test; (σενάρια, δικαιώματα)


Services Cloud
TOR Network
Internet
Corporate Office
Users
Home Office
Branch Office
INTRUSION ALERT
IPS
DMZ - Exchange
Internal servers

IT Security Audit / Extended

Αποτελεσματικό εργαλείο για την **σφαιρική προστασία** των δικτύων.

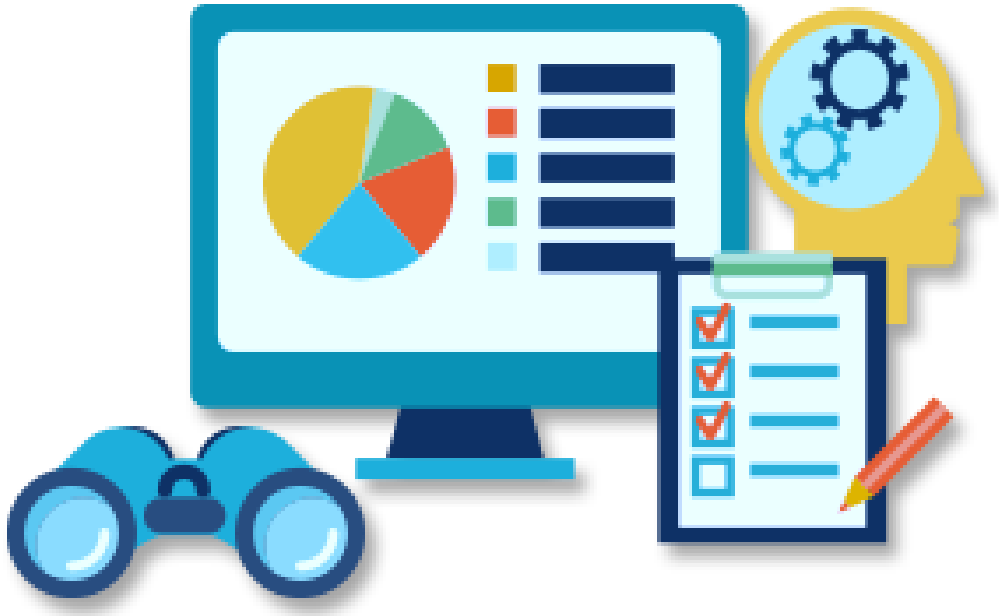
- Ελέγχονται όλα τα στοιχεία του δικτύου.
- Διαπιστώνεται ο βαθμός συμμόρφωσης σε πρότυπα, κανόνες και πρακτικές.
- Καταγράφονται προβλήματα.

Το **Extended** βασίζεται στο **NIST** και επιπλέον ελέγχει διαδικασίες που μπορεί να γίνουν αντικείμενο εκμετάλλευσης.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

IT Security Audit / Extended

- Επισημαίνεται ο κίνδυνος που προκύπτει από κάθε πρόβλημα.
- Εκτιμάται το κόστος και οι πόροι που απαιτούνται για τη διόρθωση των προβλημάτων.
- Προτείνονται τρόποι βελτίωσης.



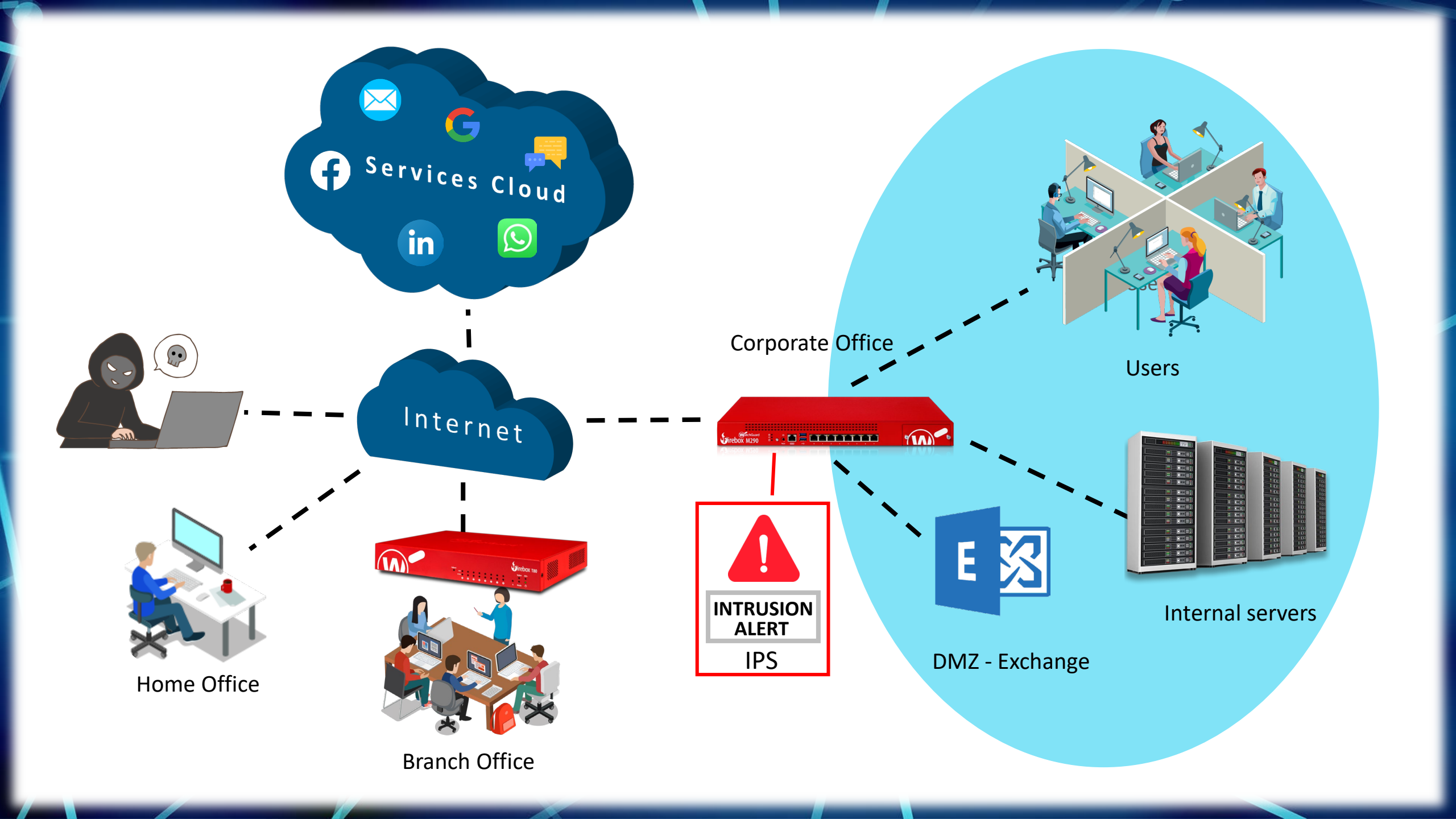
IT Security Audit / Extended

Τμήμα Report

Απαιτήσεις Ασφάλειας		level	Status	Σχόλια	Επεξήγηση
1.1	Servers που έχουν υπηρεσία προσβάσιμη από το Internet, πρέπει να συνδέονται στη DMZ.	●	YES	Mail & Web App σε DMZ	Εάν κάποιος από τους Internet Server προσβληθεί, να περιοριστεί η επίθεση και να μην μεταδοθεί στο υπόλοιπο δίκτυο.
1.2	Απαγόρευση Port Forward στο εσωτερικό δίκτυο.	●	NO	Port Forward σε DVR στο LAN	Για να αποτραπεί η εκμετάλλευση τυχόν αδυναμίας του πρωτοκόλλου που γίνεται NAT
1.3	Χρήση κρυπτογραφημένων πρωτοκόλλων για management.	●●	YES	Watchguard System Manager & HTTPs	Για να μην υποκλαπούν τα Credentials του Admin
1.4	Ενεργοποίηση κανόνων Proxy στις HTTP/HTTPs συνδέσεις.	●●	YES		Οι κανόνες Proxy είναι απαραίτητοι για αποτελεσματικό έλεγχο virus και επιθέσεων.
1.5	Ενεργοποίηση υπηρεσιών Content Filtering.	●●	YES	Εκτός από workstation διοίκησης	Όταν περιορίζεται η πρόσβαση σε αμφιβόλου φήμης Sites περιορίζονται και οι πιθανότητες μόλυνσης των Η/Υ.

Security Audit

Ποια προβλήματα του NG Firewall αναδεικνύονται στο Audit και δεν τα βρίσκει το Penetration Test.


Services Cloud
Internet
Corporate Office
Users
Home Office
Branch Office
INTRUSION ALERT
IPS
DMZ - Exchange
Internal servers

Ευχαριστούμε!

Simasecurity.gr
info@simasecurity.gr

Digitalsima.gr
sales@digitalsima.gr