Od dawna jest wiadomym, że mam w zwyczaju zaglądać na różne fora internetowe. Zadawać pytania ludziom i im na nie odpowiadać, o ile mieszczą się one w zakresie mojej wiedzy. Odkąd pierwszy raz zetknąłem się z technologia jaką jest Next-Generation Firewall zbierałem się aby napisać o tym artykuł. Aż pewnego dnia…

Aż pewnego dnia, suma wydarzeń dziejących się wokół mnie spowodowała, że miałem czas, Palo-Alto i pretekst, aby napisać kilka słów. Ale zanim cokolwiek technicznego, trochę wyjaśnień. Nazwijmy to F.A.Q do tego arta.

1. Nie, to Palo Alto nie jest moje.
2. Ceny można sprawdzić na stronie Palo Alto Networks. Jednakże należy pamiętać, że kupując u pośrednika który kupuje duże ilości u producenta, można dostać rabat.
3. Nie jest to sprzęt domowego użytku. Inaczej, można z powodzeniem używać w domu, jeżeli ktoś potrzebuje, ewentualnie współdzieli łącze z niezaufanymi osobami.
4. Najmniejsze palo to pa-200. Spokojnie nadaje się do biura.
5. Next Generation Firewall charakteryzuje się tym, że posiada możliwość blokowania ruchu na L7 (warstwa aplikacji)

Ok, myślę, że moje odpowiedzi zaspokoi większość pytań, inne można kierować do mnie. Oczywiście pamiętajcie, aby podać swój username i hasło.

Post który mnie przekonał o potrzebie napisania tego artykułu to ten zamieszczony poniżej.

Trafiłem ostatnio na sieć LAN/WLAN opartą na Cisco + Fortigate firewall, w której wycięty jest TOR.

Co znaczy wycięty:

1. Nie łączy się przy domyślnej konfiguracji.
2. Nie łączy się przy domyślnym bypass ISP blok.
3. Nie łączy się przy ręcznym dodaniu bridges (pozyskanych auto-email'em).
4. Wyjście do sieci nie używa proxy (nie na poziomie aplikacji - przeglądarki).

Zastanawia mnie co tak skutecznie wycina TORa, Cisco czy Fortigate? Jakie funkcje konkretnie są za to odpowiedzialne? Jak to ugryźć by zestawić połączenie z TORem?

Używam TOR bundlepack. Nie sprawdzałem czy port 9150 jest wycięty ani czy TOR używa domyślnie tego portu czy losowych.

LOG z TORa przy failu z użyciem brides.

KOD: ZAZNACZ CAŁY

```
2015-01-20 11:14:08.303 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down
all existing connections.
2015-01-20 11:14:08.303 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down
all existing connections.
2015-01-20 11:14:08.303 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down
all existing connections.
2015-01-20 11:14:08.303 [NOTICE] Opening Socks listener on 127.0.0.1:9150
2015-01-20 11:14:08.918 [NOTICE] Bootstrapped 5%: Connecting to directory server
2015-01-20 11:14:08.920 [NOTICE] Bootstrapped 10%: Finishing handshake with directory server
2015-01-20 11:19:08.880 [WARN] Problem bootstrapping. Stuck at 10%: Finishing handshake with directory server. (DONE; DONE; count 1;
recommendation warn)
2015-01-20 11:19:08.880 [WARN] 1 connections have failed:
2015-01-20 11:19:08.881 [WARN]  1 connections died in state handshaking (TLS) with SSL state SSLv2/v3 read server hello A in
```

Oczywiście, zaskoczyło mnie, że ktoś posiadający wiedzę, iż znajduje się w sieci zabezpieczonej za pomocą cisco i fortigate, zamiast użyć googla i dowiedzieć się co nieco o temacie, zadaje pytania na forum. No cóż, widocznie niektórych google boli.

W tytule wspomniałem POPR'a, kto śledzi w jakikolwiek moja działalność na IRC, na pewno spotkał się już z tym określeniem, jeżeli nie – Linkuję.

Jak można się domyślić po opisie POPR'a, jest to człowiek utrudniający życie użytkownikom (spojrzenie od strony użytkowników), natomiast ja uważam, że jest to osoba, która poważnie traktuje swoja pracę. Oczywiście nie mówię o POPR'ze z opowiadań. POPR z opowiadań to po prostu znudzony psychol w pracy jakich wielu. Dzisiaj, do postaci administratora z opowiadań porównuję się bezpieczników czy ogólnie adminów zarządzających sekcjami dostępu lub stykiem sieci z internetem. Dlaczego? Odpowiedź na to pytanie jest prosta. Do ich obowiązku należy zapewnienie sieci jak najwyższy poziom bezpieczeństwa i „jak najniższą ilość czerwonych komunikatów" (określenie „jak najniższa ilość czerwonych komunikatów" jest tłumaczona jako „święty spokój". Określenie to, usłyszałem od znajomego adminów, gdy Ci składali sobie świąteczne życzenia). Rozwiązania są dwa. Jedno proste, ale nieskuteczne. Drugie, mozolne, ale w końcowym efekcie mające upragniony efekt braku czerwonych komunikatów.

Sposób pierwszy.

Oczywiście, można by wyłączyć blokowanie, torentów, tora, vpn'ów czy wychodzące ssh. Oczywiście, będziemy wtedy cieszyć się spokojem. Do pierwszej kontroli szefostwa, lub pentestów (zamówionych lub nie).

Sposób drugi.

Stajemy się POPR'em i konsekwentnie blokujemy cały niepożądany ruch. Simple is not it? Nope! A teraz do sedna…

Czas na wikisekcje:

```
Zapora sieciowa (ang. firewall – ściana przeciwogniowa) – jeden
ze sposobów zabezpieczania
sieci i systemów przed intruzami. Termin ten może odnosić się zarówno
do dedykowanego sprzętu
komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego
oprogramowania blokującego
niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę
połączenia ochrony sprzętowej
i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz tzn.
sieci publicznych, Internetu,
chroni też przed nieuprawnionym wypływem danych z sieci lokalnej
na zewnątrz. Często jest to
komputer wyposażony w system operacyjny (np. Linux, BSD) z odpowiednim
oprogramowaniem.
Do jego podstawowych zadań należy filtrowanie połączeń wchodzących
i wychodzących oraz
tym samym odmawianie żądań dostępu uznanych za niebezpieczne.
```

Cóż, dziś myślę, że nie muszę tłumaczyć tego co w wikisekcji. Jedynie krótko podsumuję. Większość z czytelników tego posta na codzień ma styczność z typowymi zaporami sieciowymi, które działają, w mojej ocenie, dosyć upośledzony. Aby omówić działanie nextgeneration firewall, musimy przytoczyć jakiś przykład. Załóżmy więc sytuacje biurową – moja ulubioną, największe pole do popisu.

Poniższe literki dotyczą sytuacji biurowej, gdzie w sieci znajduje się około 20-30 osób, a nie serwerowni, gdzie stosuję się bardziej zaawansowane firewalle starego typu niż użyty przeze mnie. Nie mniej, przykład ten jest oparty na tych samych mechanizmach działania i po uprzednim zmodyfikowaniu względem sytuacji może być stosowany jako przykład dla większych sieci.

Wytyczne:

Administrator ma obowiązek wynikający z regulaminu firmowego obserwacji ruchu, aby wykrywać i zgłaszać naruszenia dotyczące odwiedzania stron www, połączeń z serwerami nie należącymi do firmy w godzinach pracy.

Co to znaczy?

Facebook, gmail, torenty, vpn, ssh są zabronione

Co robi admin?

Admin, który ma zwykły firewall po swojej stronie, pierwszym co robi, to łapie się za głowę, bo wie, że czeka go trochę pracy. Może wyciąć ruch na zewnątrz po następujących portach: wszystkie prócz 80 i 443. Oczywiście nie uda mu się wyciąć w ten sposób torenty, vpn, i ssh. A co z Facebookiem i gmailem?

Standardowy firewall pozwala nam na blokowanie ruchu po IP oraz portach.
Co w przypadkach, w których użytkownik zmienił konfiguracje ssh/vpn?

W tym momencie, najczęściej dużo nie zrobimy. I znów musimy siedzieć i selekcjonować dane do raportów.

Natomiast admin posiadający w swoim władaniu palo może wiele. Zacznijmy od tego,

że nasz firewall, w tym konkretnym przypadku użyjemy Palo-Alto 3020. Podaruję sobie opowiadanie o specyfikacji (dostępna na stronie palo). Dziś zajmiemy się kwestiami podstawowej konfiguracji.

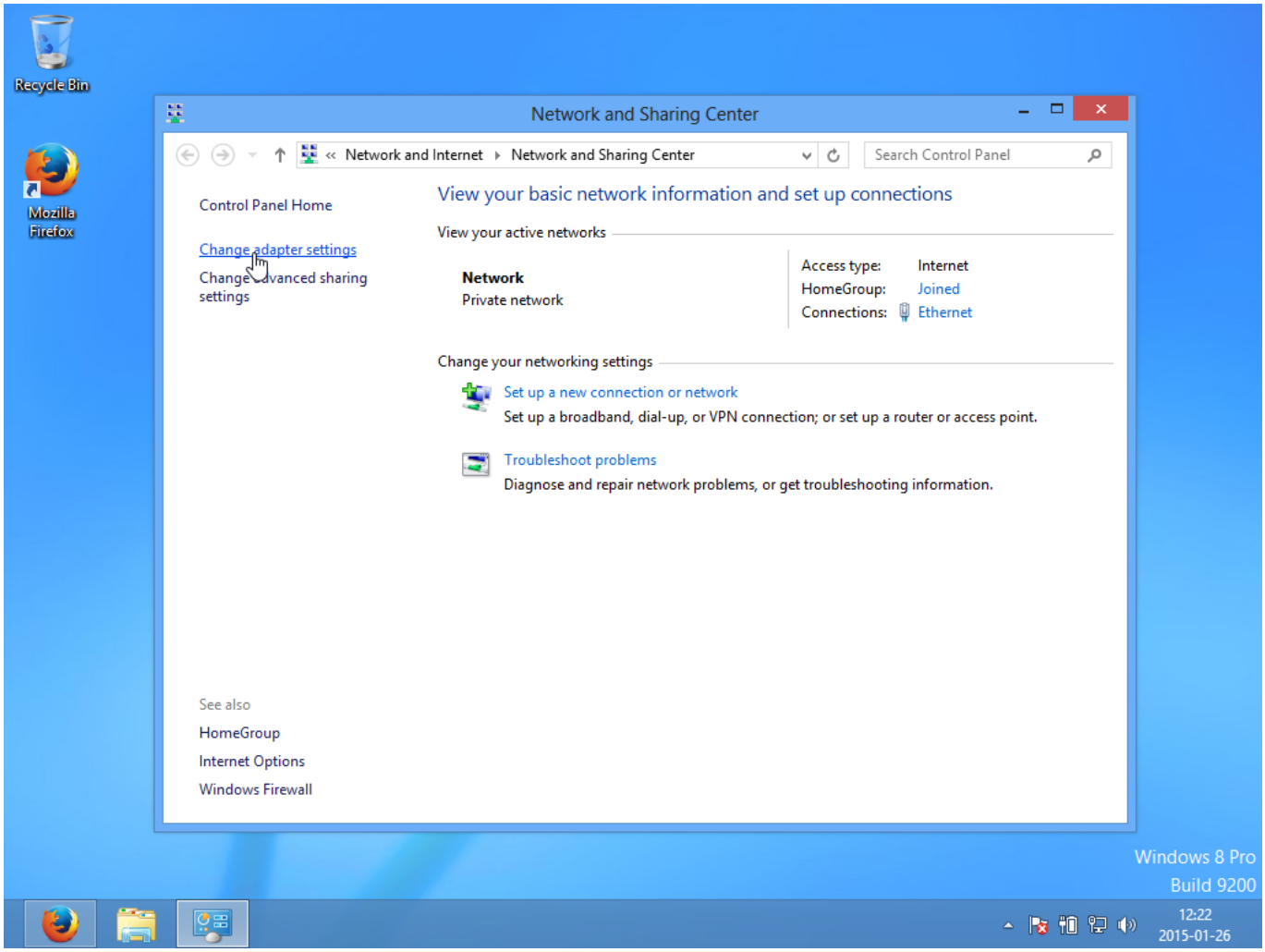
Co będziemy robić?

1. Nawiązanie połączenia z Palo Alto
2. Zaadresujemy port na którym damy dostęp do zarządzania,
3. Zaktualizujemy sygnatury aplikacji na palo oraz wersje systemu.
4. Stworzymy sieć w której będzie pracował user przed wdrożeniem palo oraz po.
5. Zgodnie z specyfikacją zablokujemy możliwość korzystania z ssh, tora, openvpn, bittorent na stardowym firewallu korzystając z routera ON NETWORKS N300. Będzie on symulował standardowy firewall
6. Umieścimy na styku sieci Palo Alto. Będzie ono pracowało jako transparentny bridge warstwy drugiej.
7. Korzystając z aplipedii Palo Alto określimy, co musimy wpisać do regułek blokujących
8. Zgodnie z specyfikacją zablokujemy konkretne usługi używając Palo Alto
9. Dokonamy obserwacji efektów.
10. Odtworzymy sytuacje z posta, w której wycięty jest tor i omówimy ewentualne metody ominięcia zabezpieczenia w celu dostania się do sieci tor.
11. Omówimy metody zapobiegania naruszeniom wspomnianych w punkcie 10.

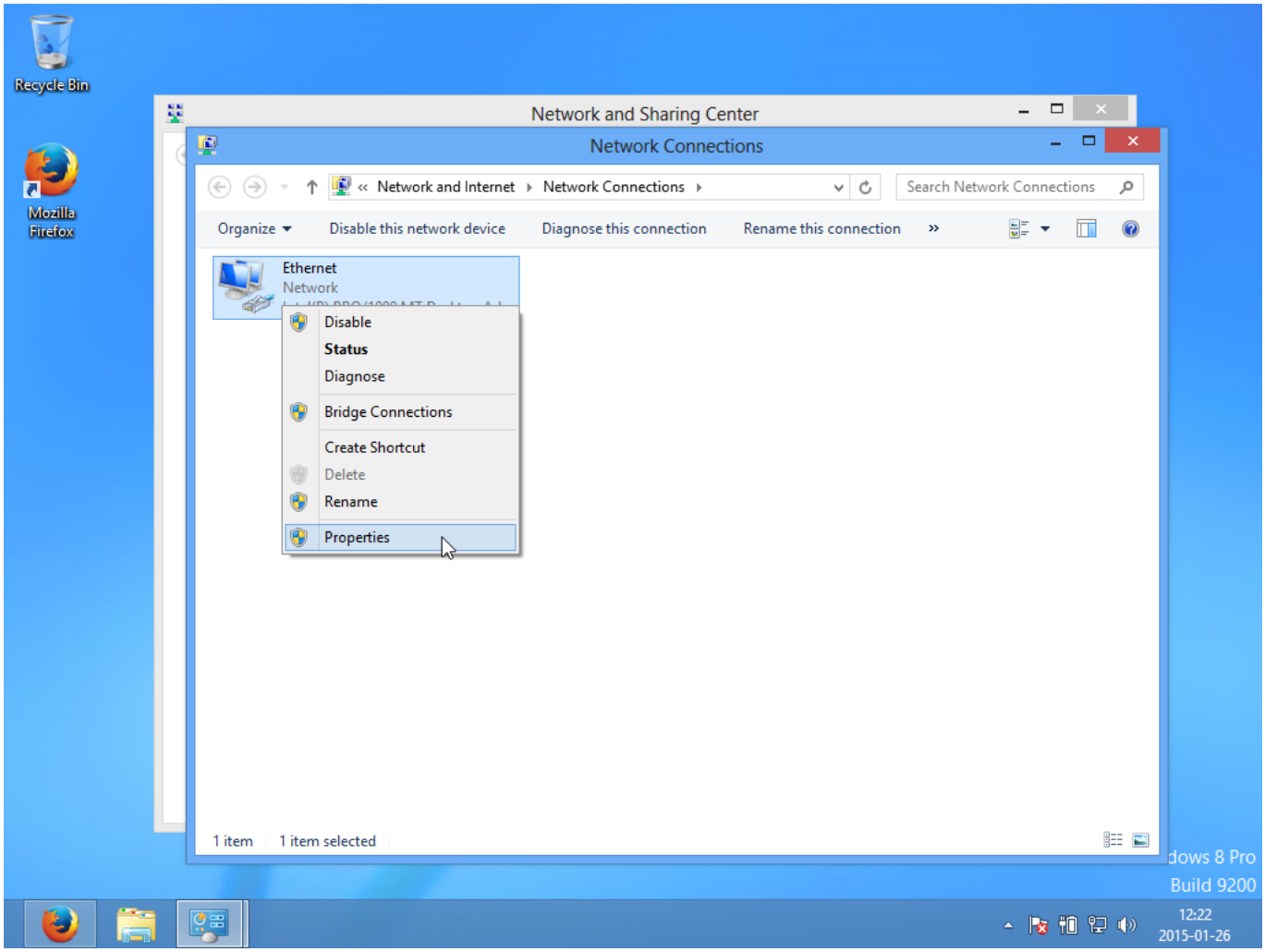
To tyle teorii na chwile obecną. Czas zacząć przygotowywaniu sprzętu.

Informacje prze zemnie podawane znajdują się w manualach dostępnych na stronach Palo Alto Networks. Gorąco zapraszam do zapoznania się z nimi.

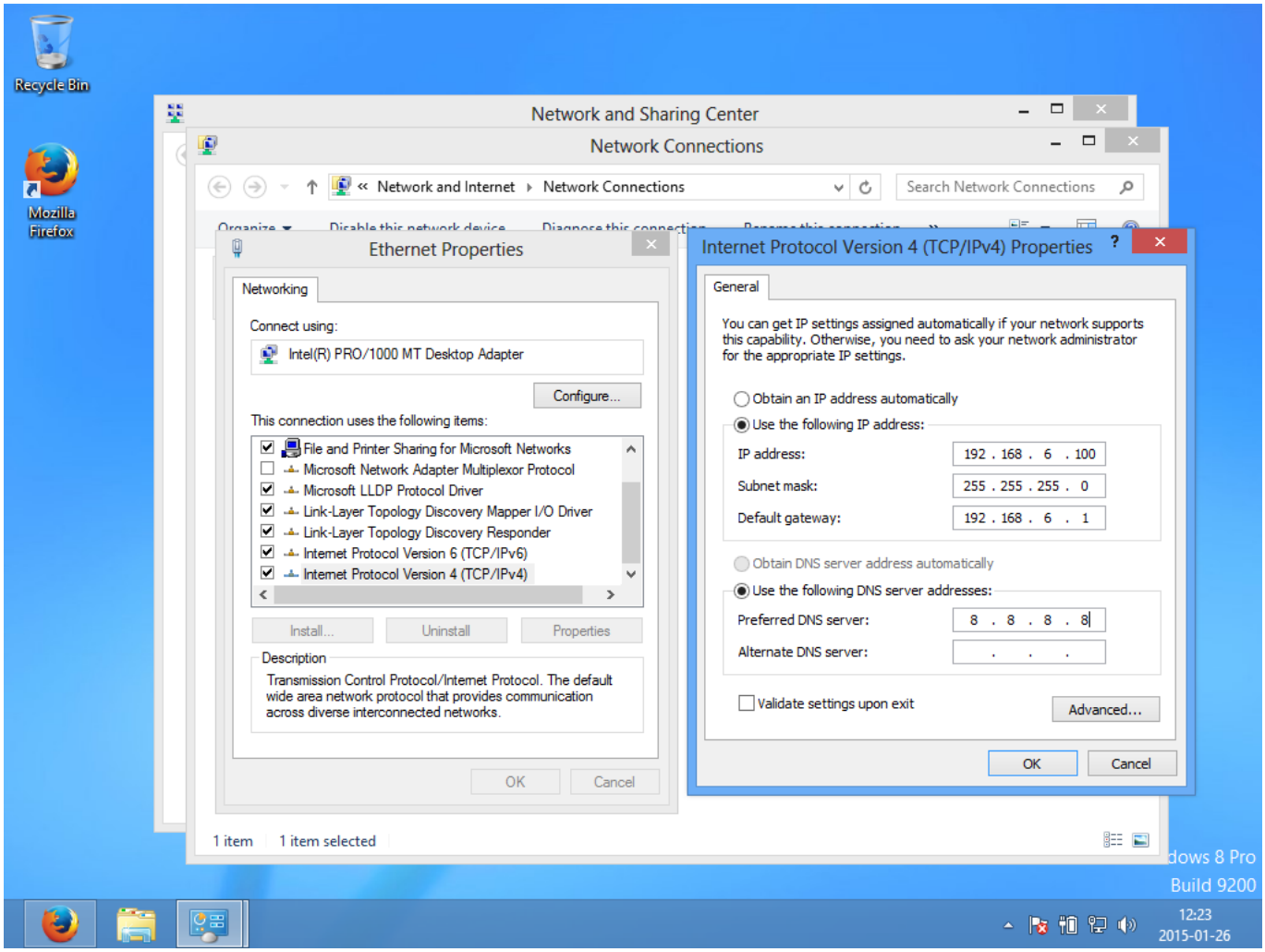
1. Nawiązanie połączenia z Palo Alto



Otwieramy Centrum Sieci i Udostępniania uruchamiamy okno edycji ustawień kart sieciowych.



Klikamy prawym na naszym porcie ethernet i wybieramy „Właściwości"



Następnie modyfikujemy ustawienia protokołu IPv4. U mnie są to:

- IP Adres 192.168.6.100
- Maska Sieciowa 255.255.255.255
- Brama Sieciowa 192.168.6.1
- DNS 8.8.8.8

Spowodowane jest to tym, że mam już wcześniej skonfigurowane palo. Standardowo należy podać dane:

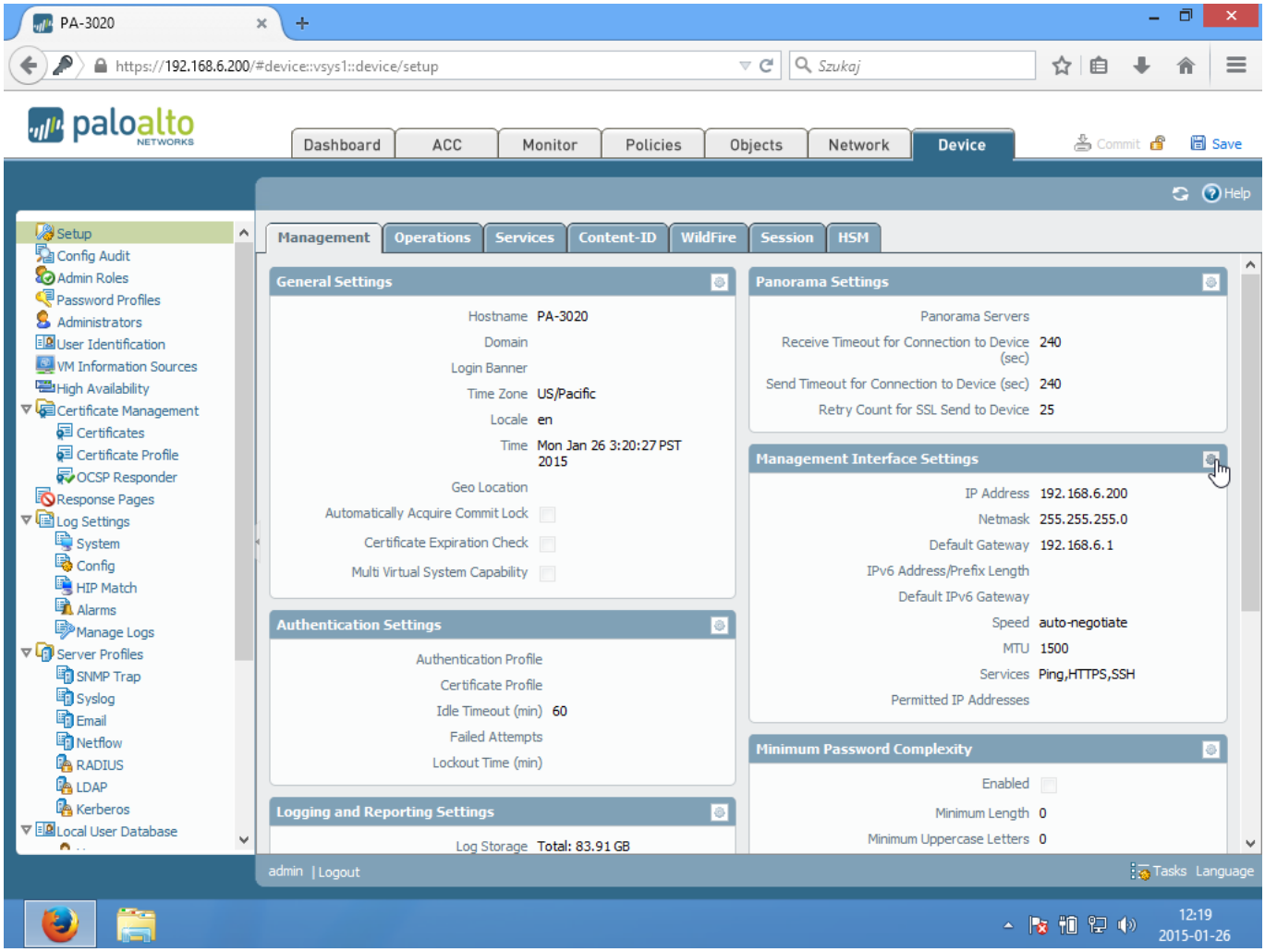
- IP Adres 192.168.1.2
- Maska Sieciowa 255.255.255.255
- Brama Sieciowa null
- DNS null

Następnie połączyć kablem ethernetowym port naszego komputera z portem zarządzania (MGT) Palo.

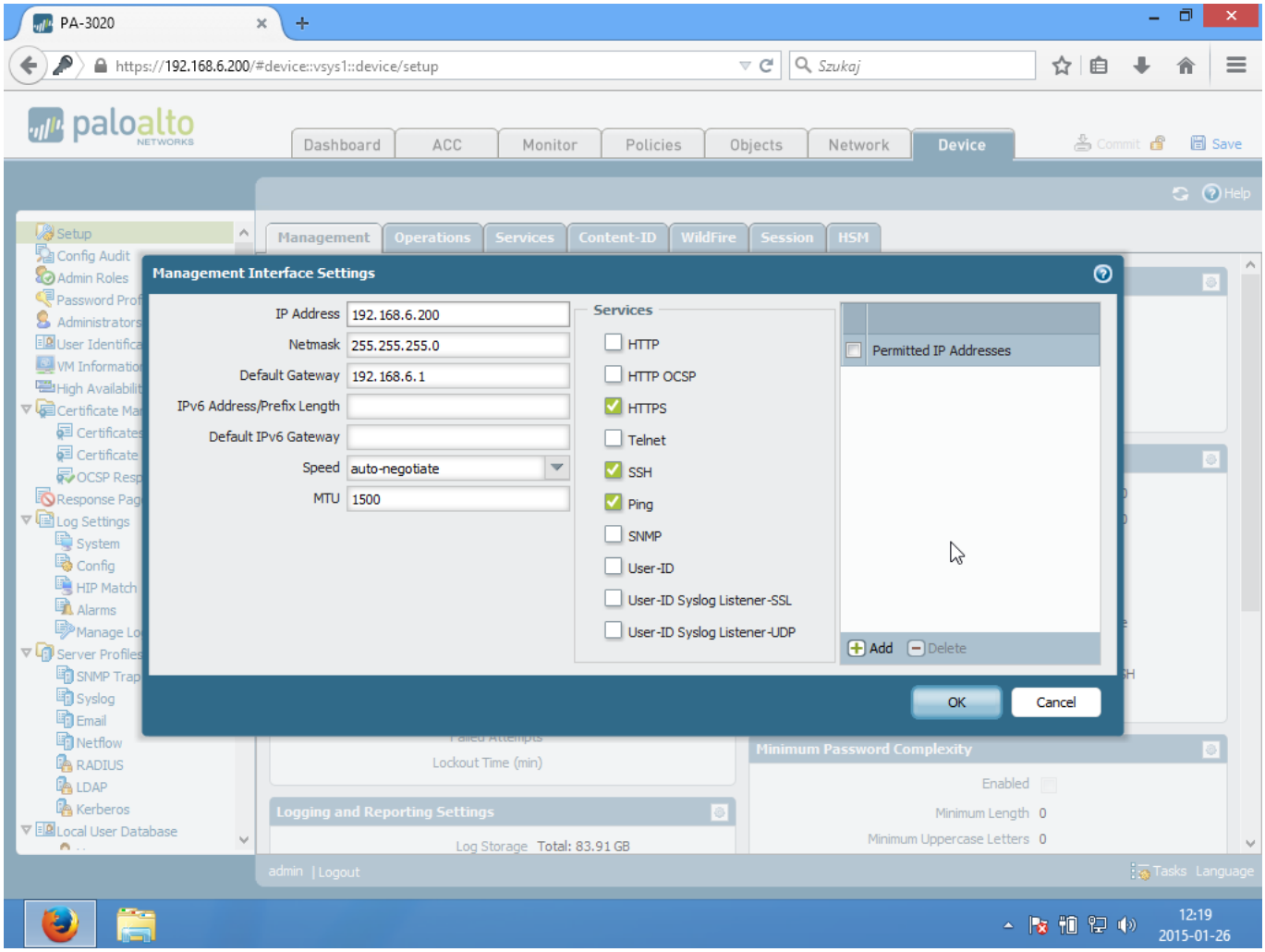
2. Adresacja portu zarządzania, podłączenie do sieci internet.

Domyślnym panelem zarządzania jest https://192.168.1.1. U mnie jest to natomiast https://192.168.6.200. Domyślny login i hasło to admin:admin. Zaleca się zmianę, tego jednak nie będę robił ponieważ jest to palo testowe a nie produkcyjne.

Obecnie, jeśli właśnie konfigurujecie jakieś palo większe niż seria 200, to pewnie obok niego stoicie i cierpicie z względu na szum, który generuje. Przejdźmy zatem najpierw do zaadresowania i podpięcia managementu do sieci w której jesteśmy podpięci po wifi. W ten sposób dalsza konfiguracje przeprowadzimy siedząc przy naszym wygodnym biurku.



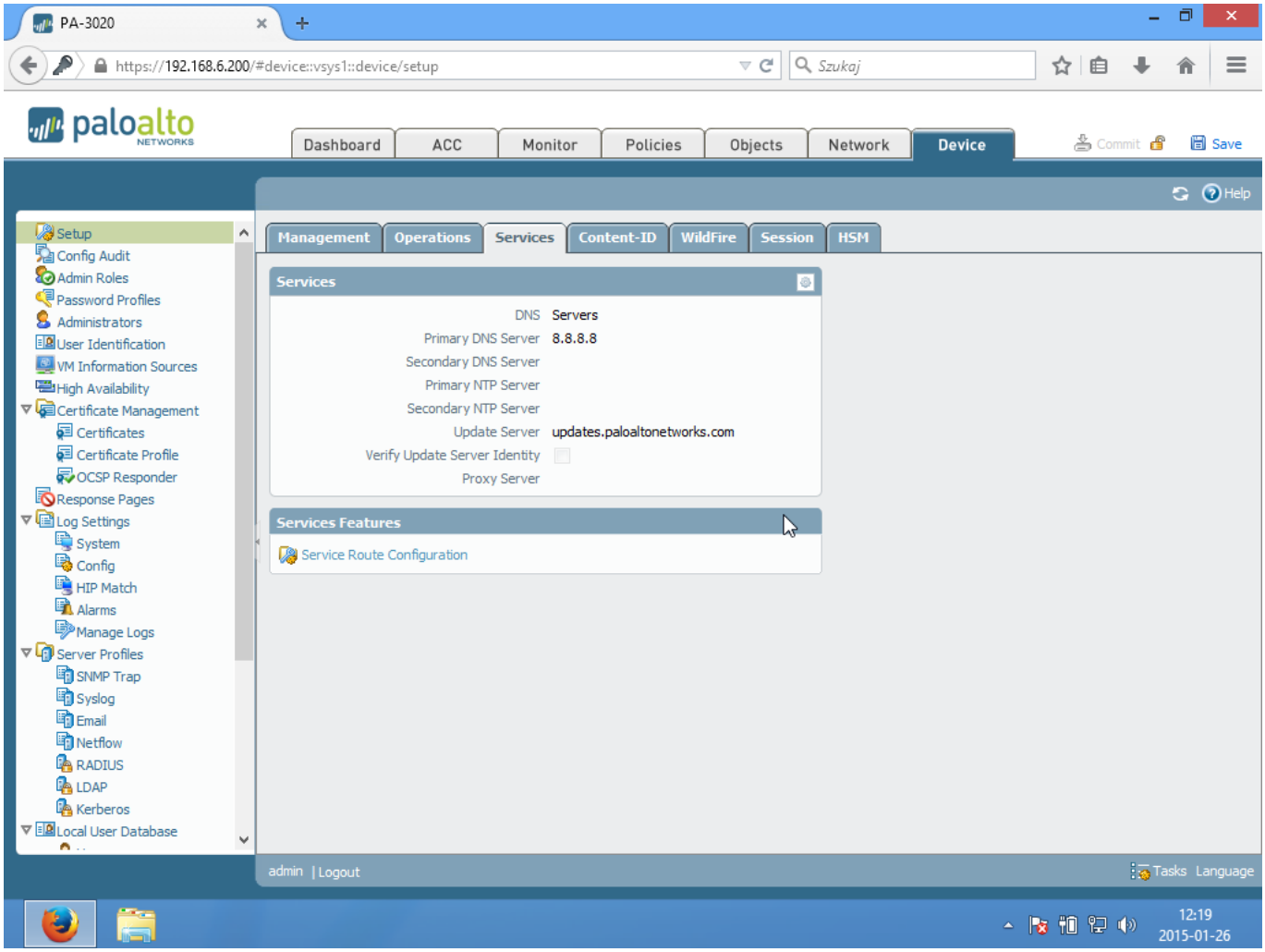
Aby zaadresować port MGT, należy wejść w zakładkę Device -> Management, następnie klikamy tak jak na obrazku.



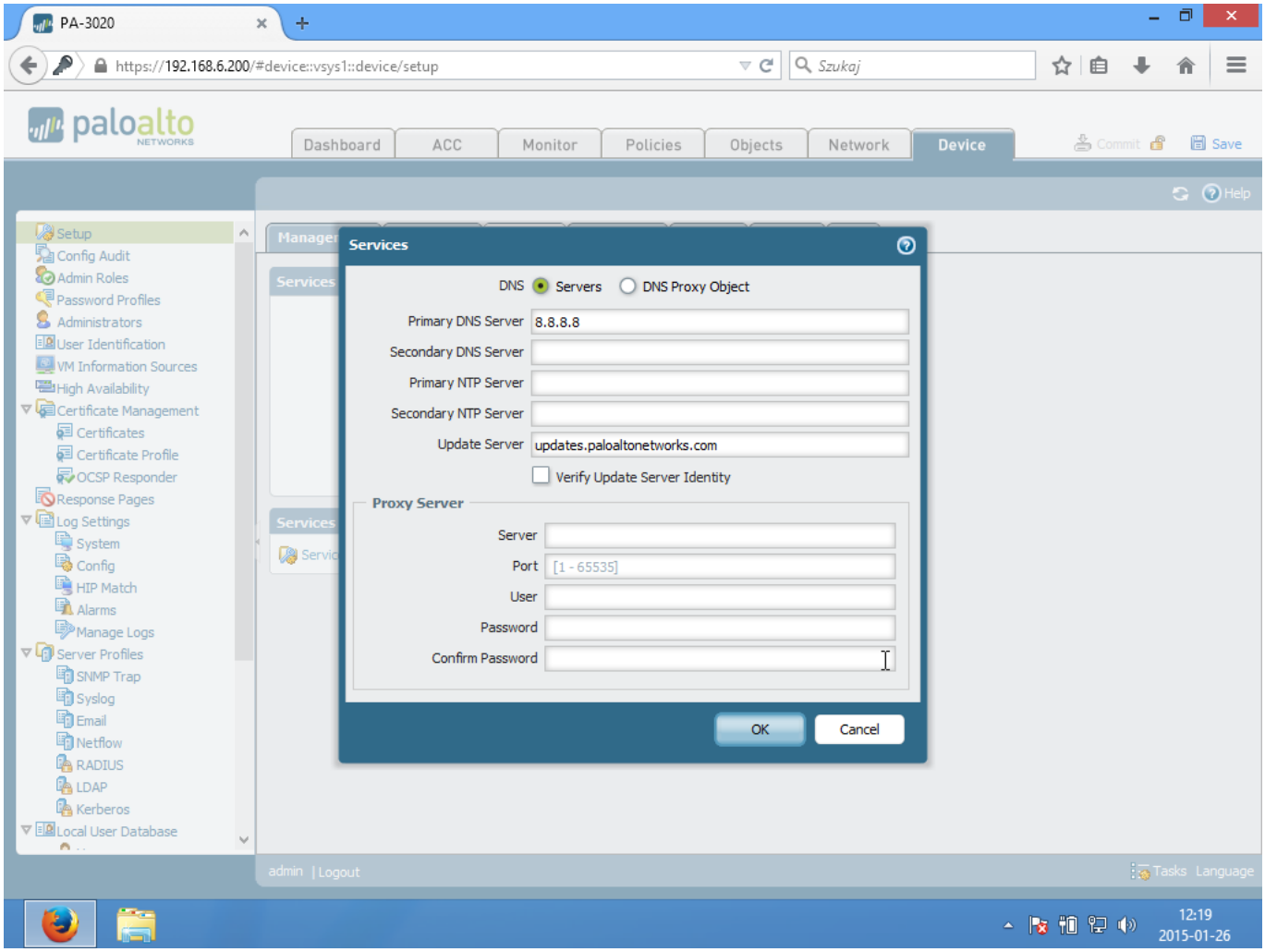
Tutaj ustawiamy adresacje portu MGT. Aby dokonać aktualizacji musimy podłączyć MGT do sieci internet. Adresujemy tak, by umożliwić podłączenie do naszej sieci.

- IP Adres 192.168.6.200
- Maska 255.255.255.255
- Brama 192.168.6.1

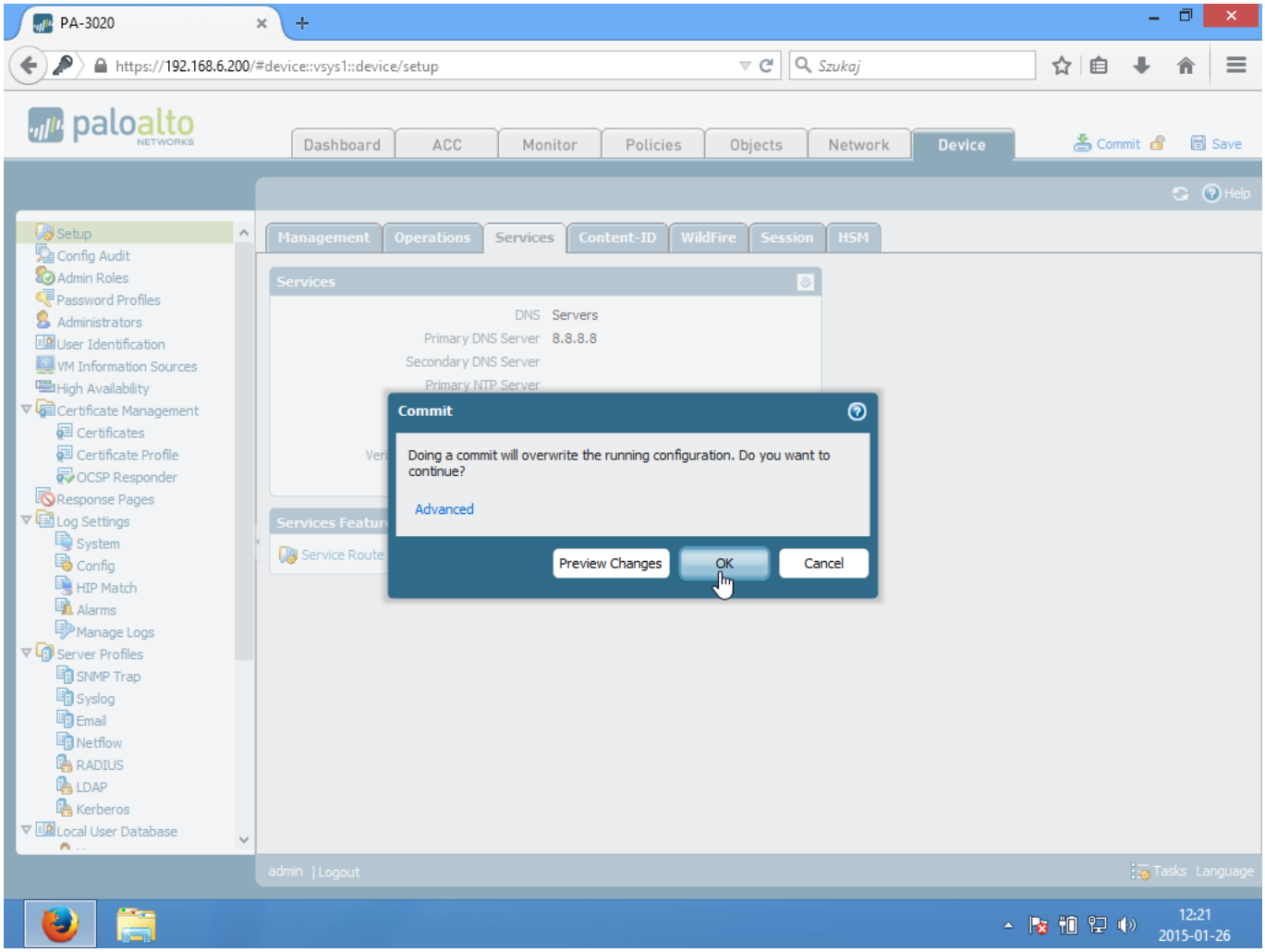
Klikamy ok i przechodzimy dalej.



W zakładce Device -> Service ustawiamy serwery DNS.



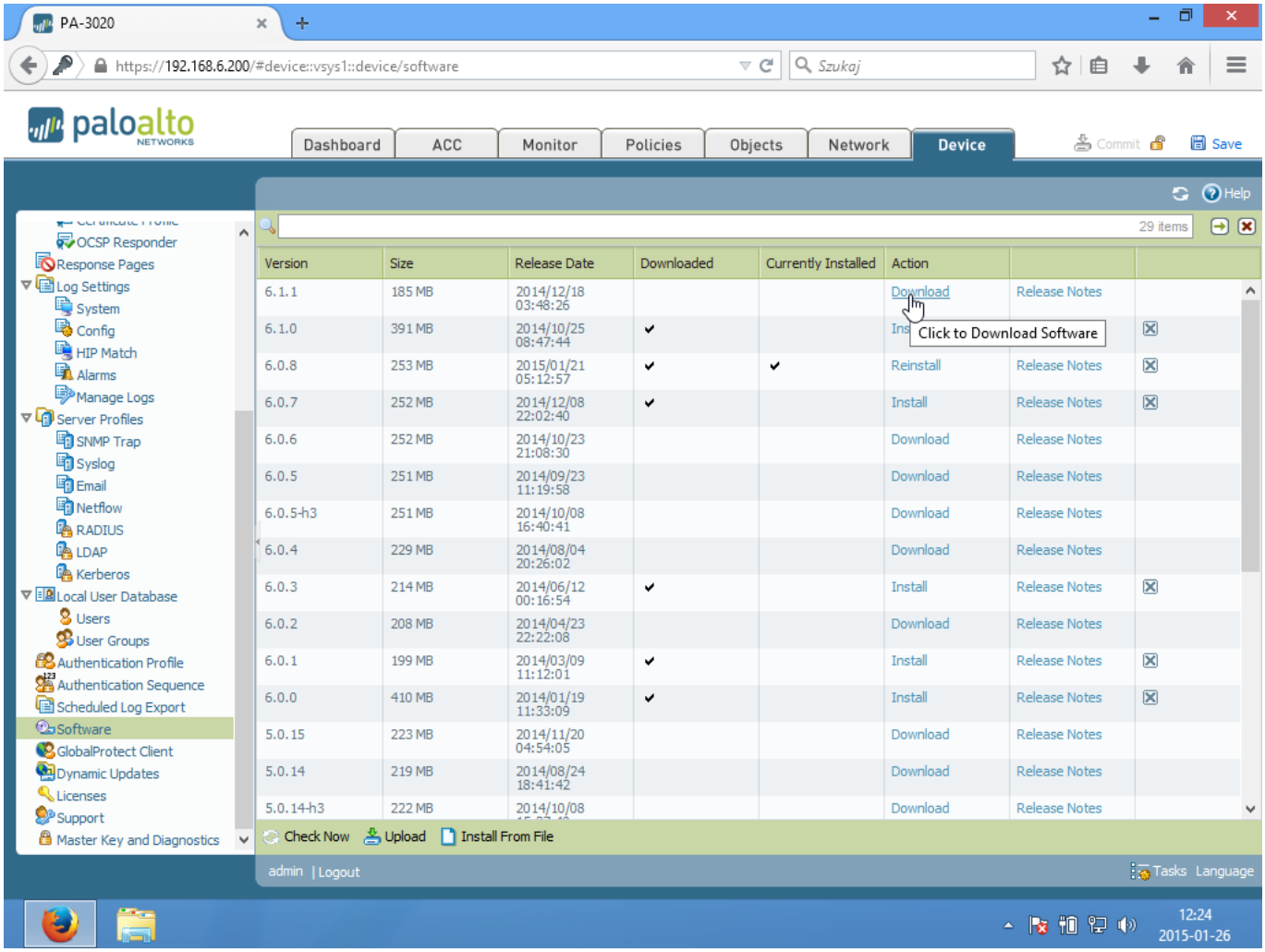
Klikamy ok i idziemy dalej.



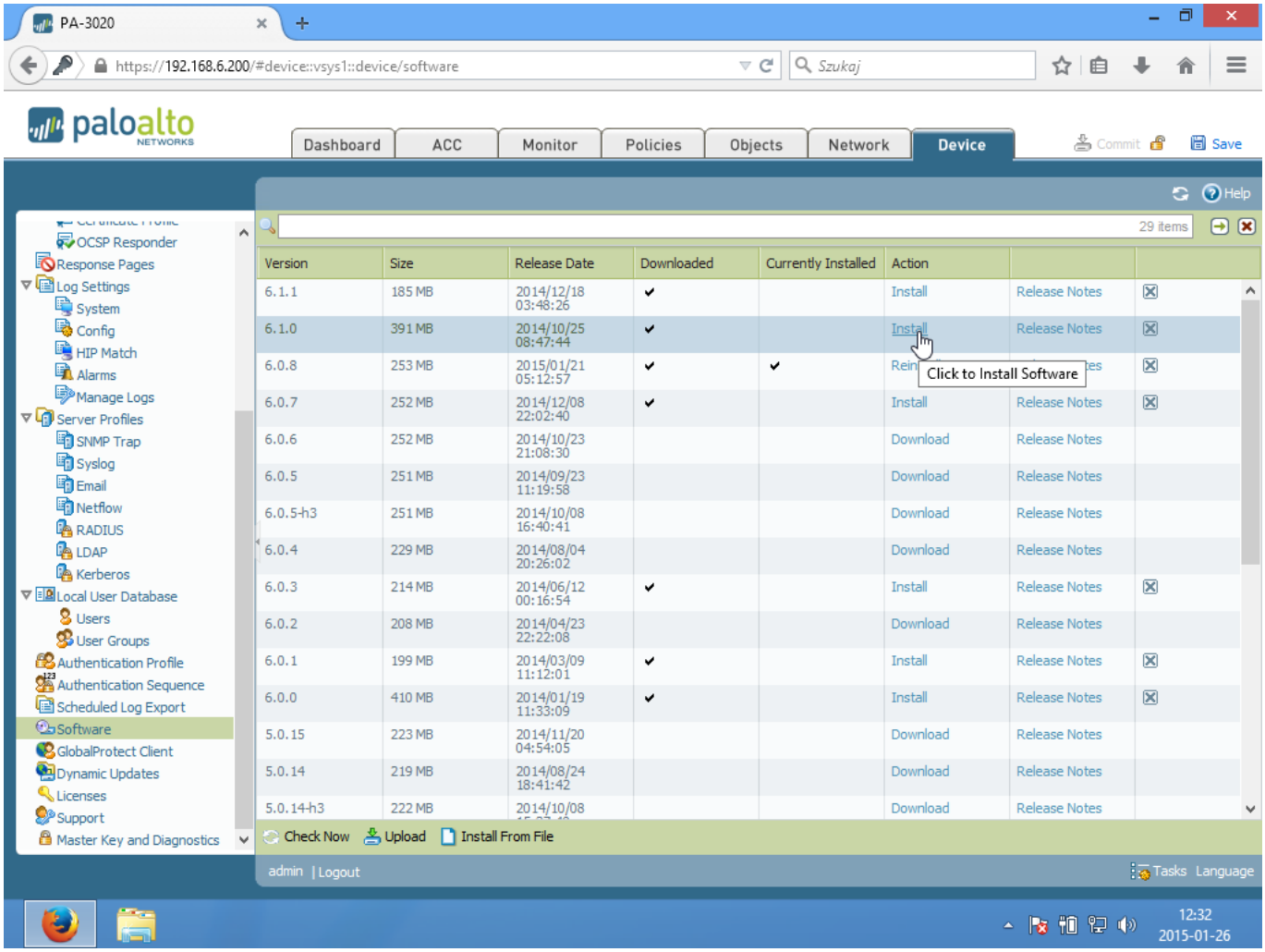
W prawym górnym rogu znajdziemy opcje „Commit" w ten sposób wcielamy konfiguracje w życie.

3. Aktualizacja systemu oraz sygnatur aplikacji.

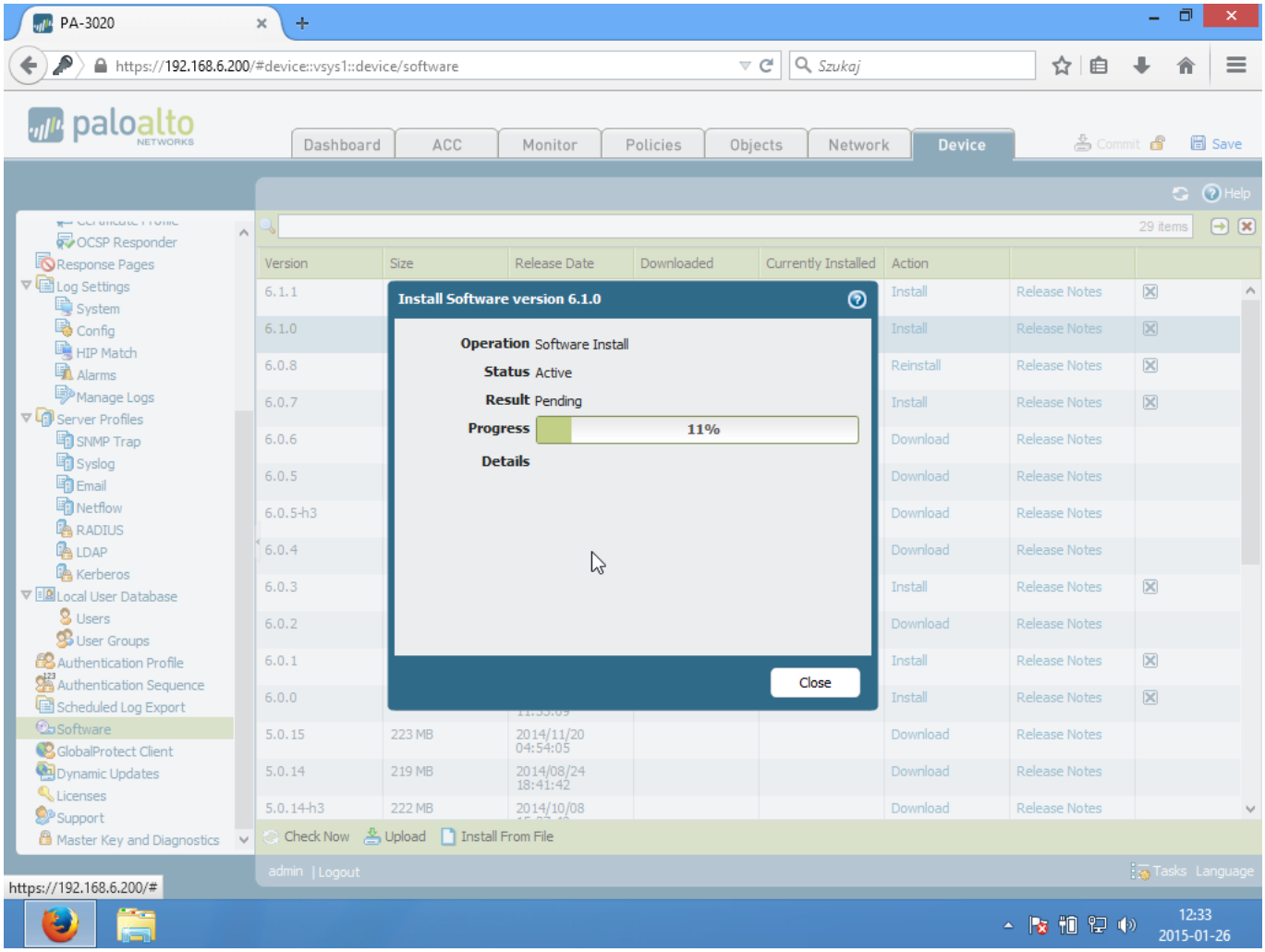
Aby nasz firewall poprawnie funkcjonował należy go zaktualizować. W tym celu przechodzimy do Device -> Software i pobieramy aktualna wersje systemu.



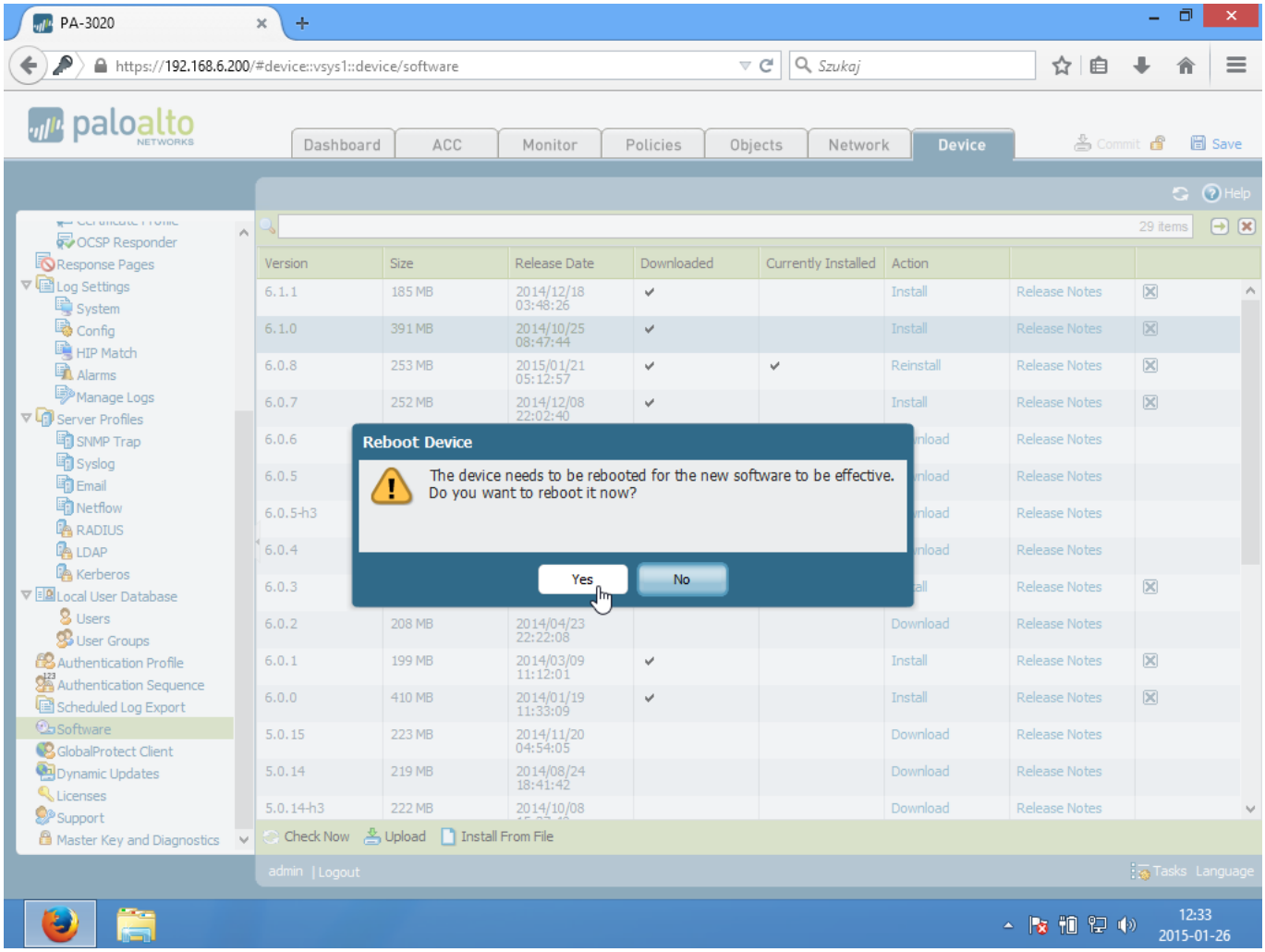
Uwaga! Wersje należy aktualizować kolejno, tak jak w tym przypadku do 6.1.0 a dopiero potem do 6.1.1.



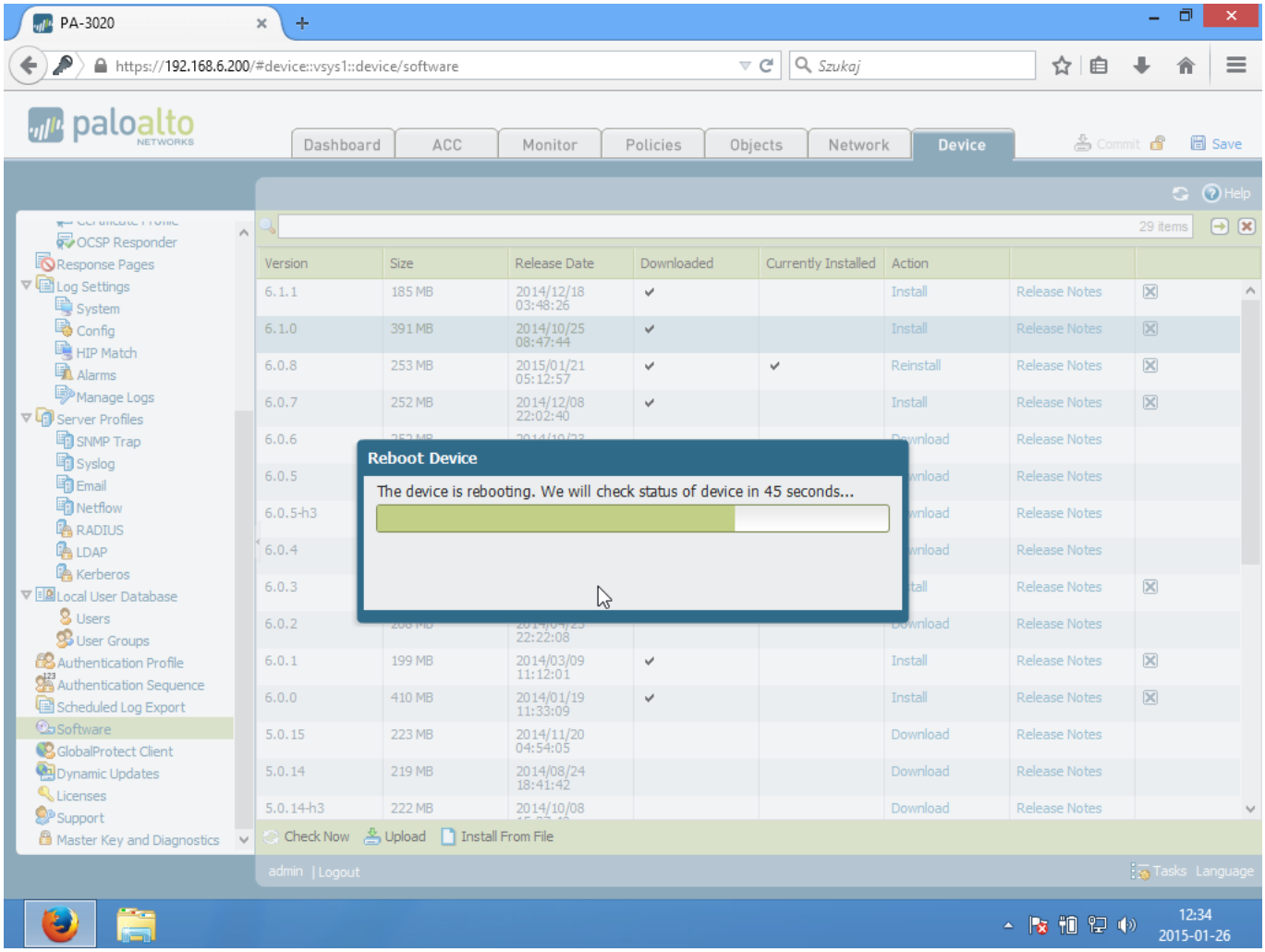
Przed instalacja, dobrze jest kliknąć „Check" w lewym dolnym rogu. To pozwoli nam pobrać aktualna listę wersji systemu. Następnie klikamy „Install".



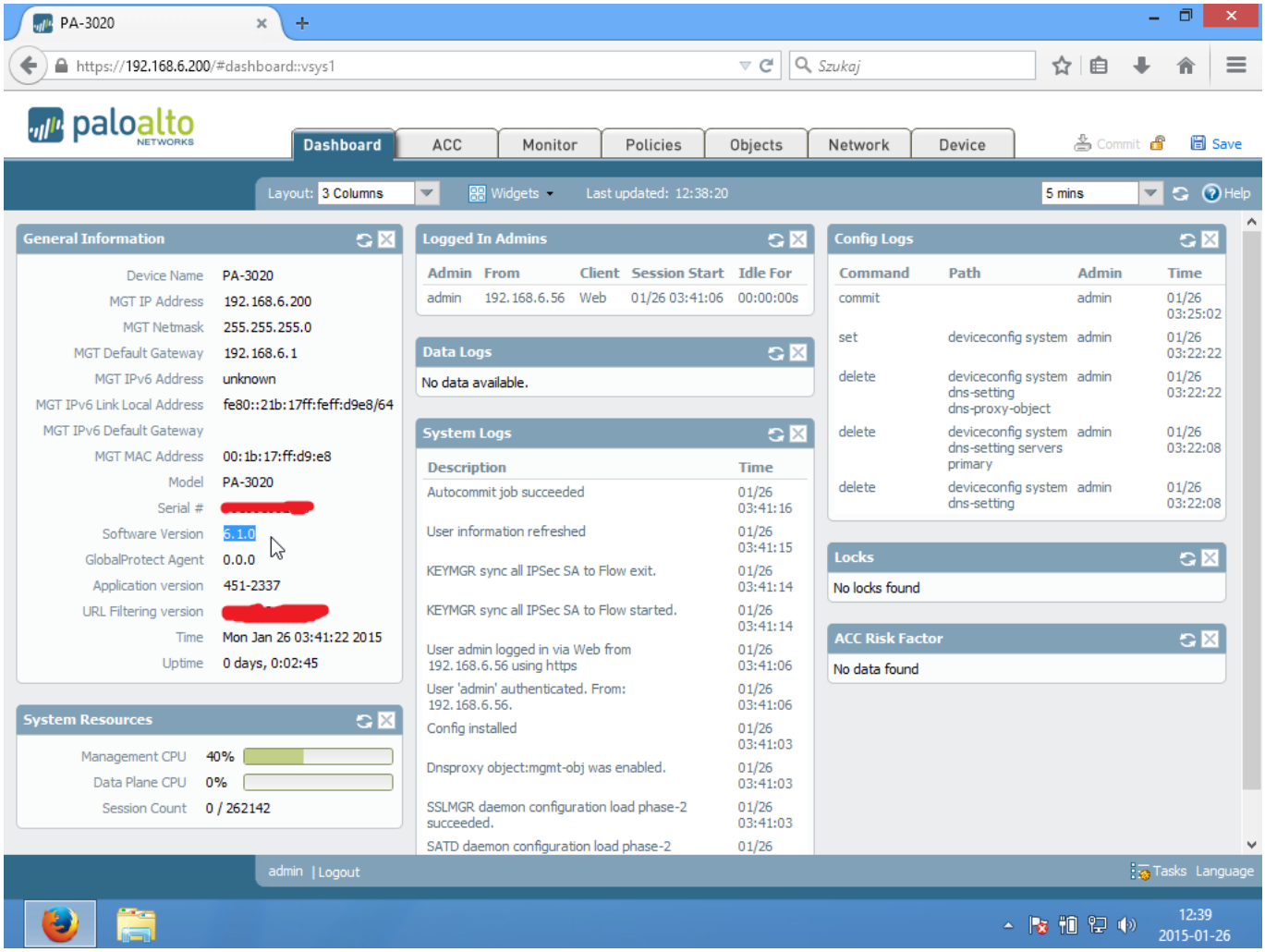
Gdy instalacja się zakończy, ponownie uruchamiamy nasze palo.

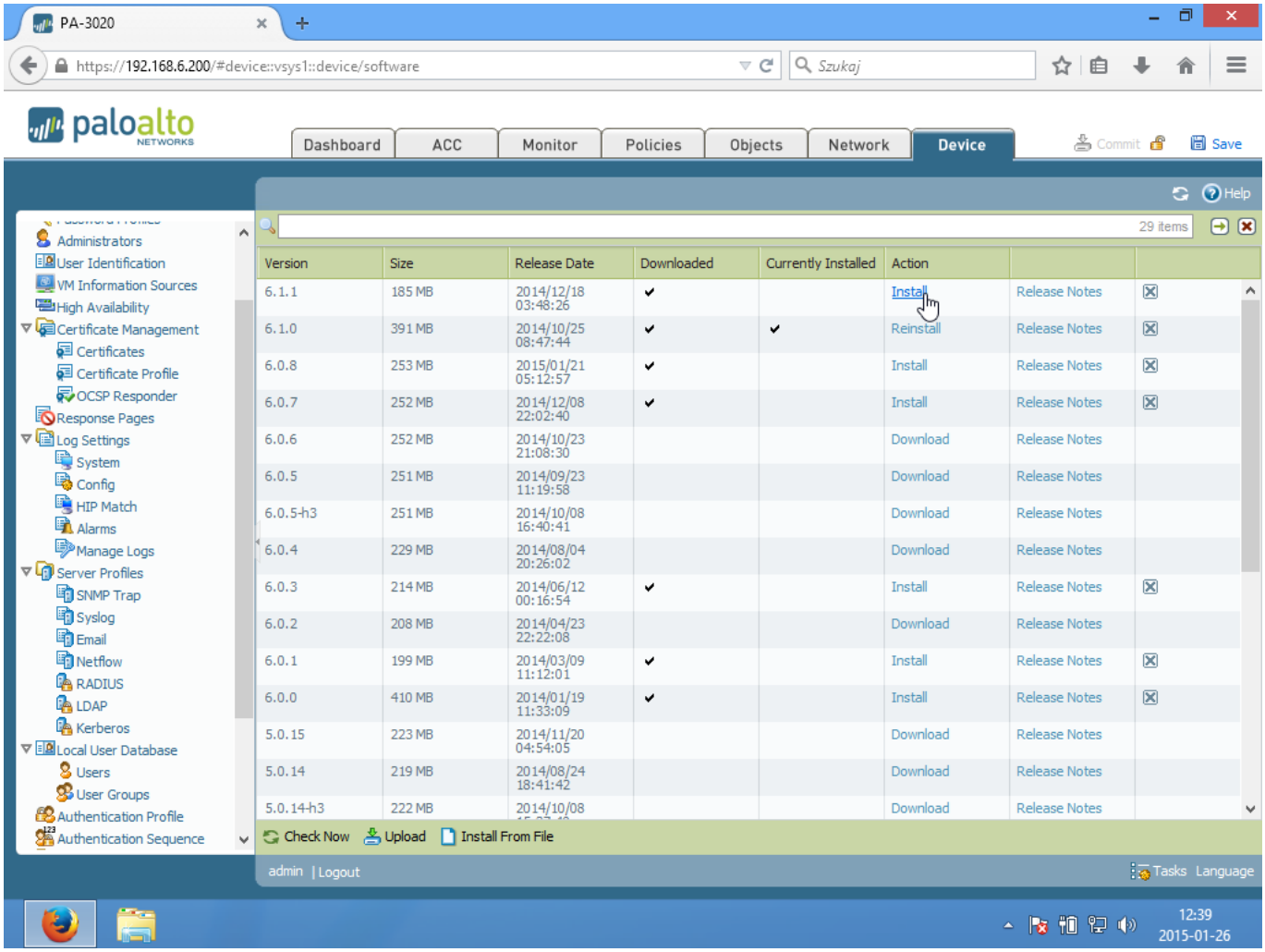


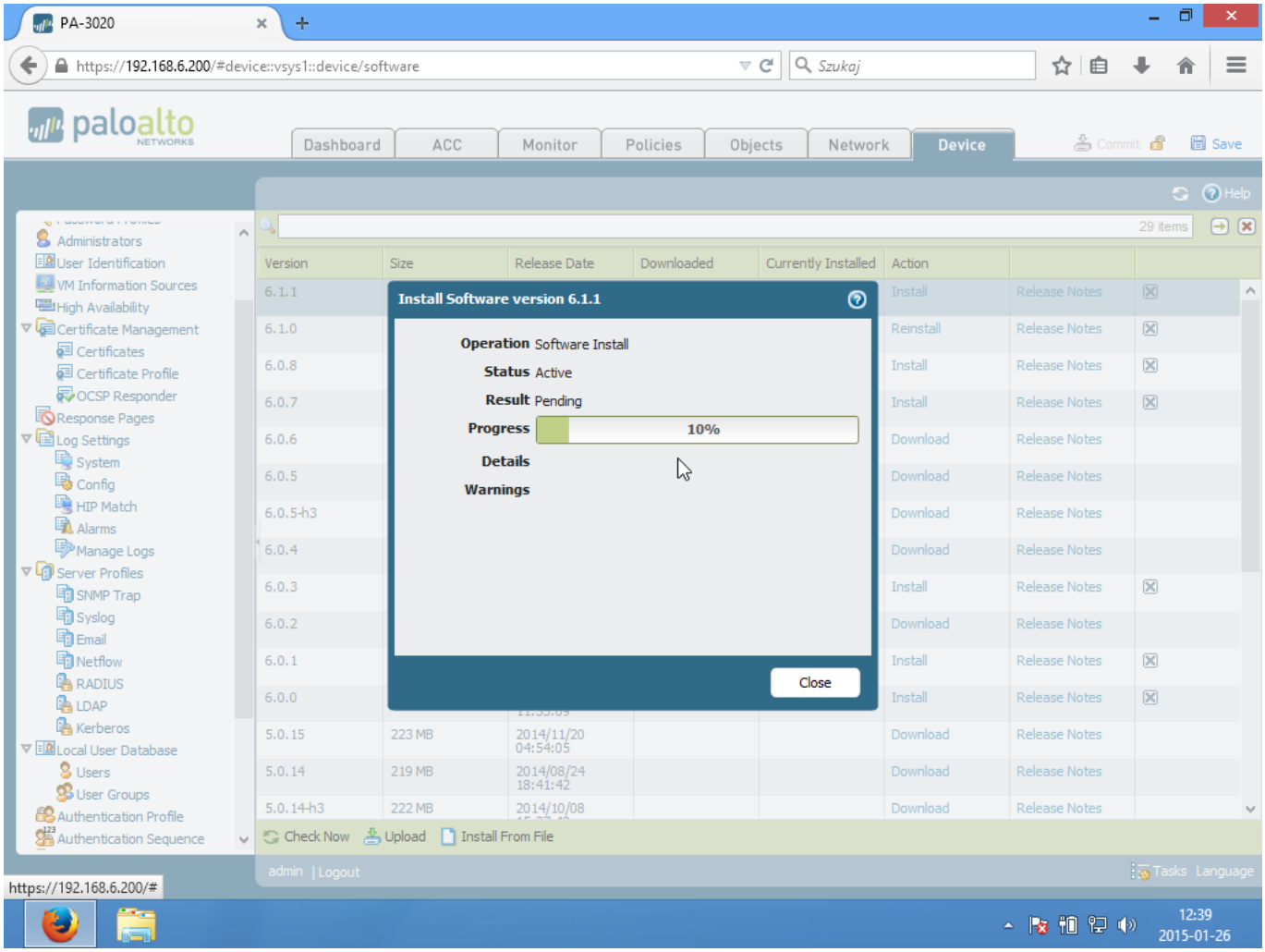
Następnie chwila oczekiwania na restart, palo samo załaduje panel logowania gdy będzie gotowe.



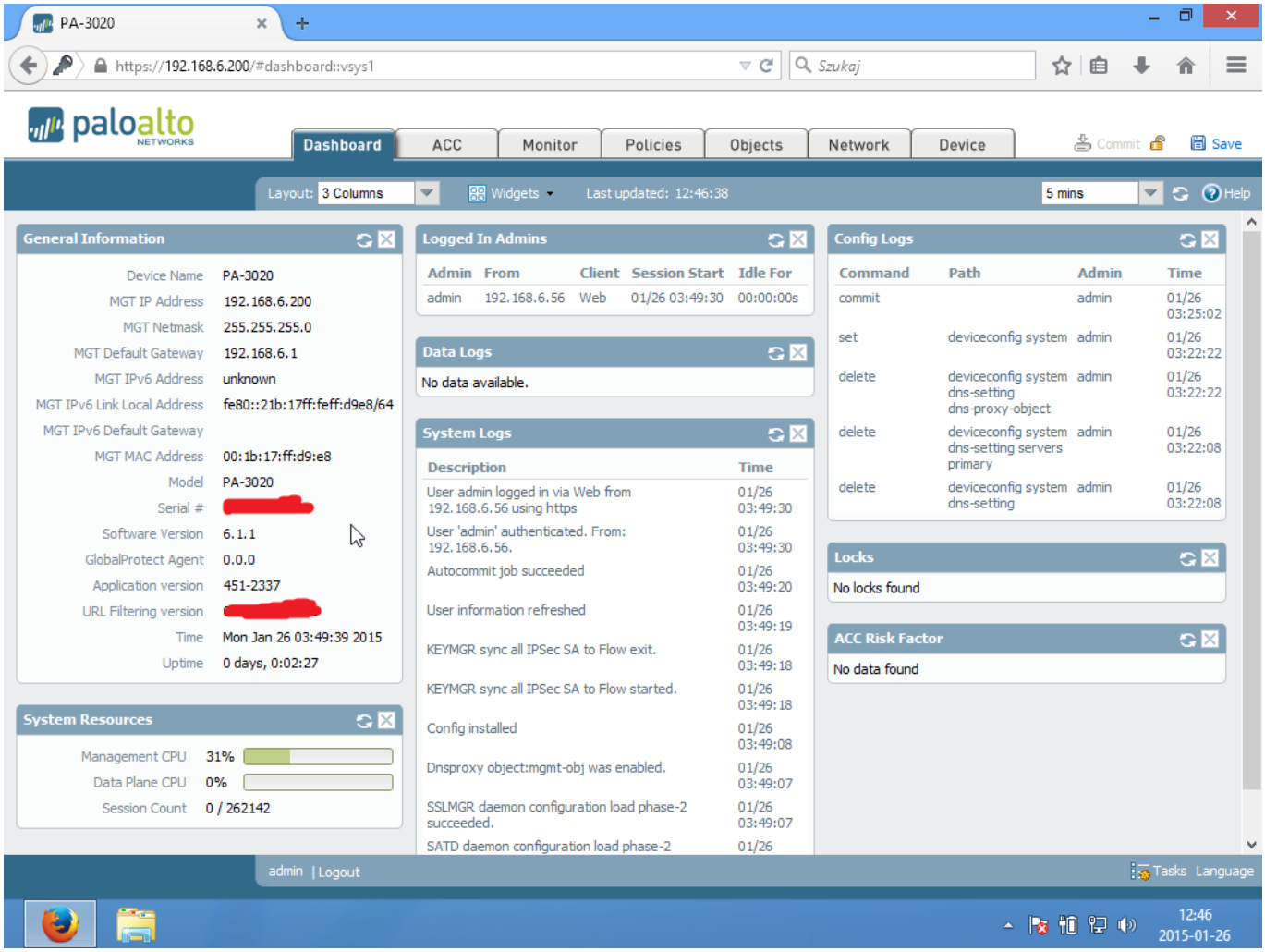
Jak widzimy poniżej, zainstalowaliśmy wersje 6.1.0. Teraz należny ponowić zabieg instalacji dla wersji 6.1.1


PA-3020
https://192.168.6.200/#dashboard::vsys1
Szukaj
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Save
Layout: 3 Columns
Widgets
Last updated: 12:38:20
5 mins
Help
General Information
Device Name PA-3020
MGT IP Address 192.168.6.200
MGT Netmask 255.255.255.0
MGT Default Gateway 192.168.6.1
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::21b:17ff:feff:d9e8/64
MGT IPv6 Default Gateway
MGT MAC Address 00:1b:17:ff:d9:e8
Model PA-3020
Serial #
Software Version 6.1.0
GlobalProtect Agent 0.0.0
Application version 451-2337
URL Filtering version
Time Mon Jan 26 03:41:22 2015
Uptime 0 days, 0:02:45
Logged In Admins
Admin From Client Session Start Idle For
admin 192.168.6.56 Web 01/26 03:41:06 00:00:00s
Data Logs
No data available.
System Logs
Description Time
Autocommit job succeeded 01/26 03:41:16
User information refreshed 01/26 03:41:15
KEYMGR sync all IPSec SA to Flow exit. 01/26 03:41:14
KEYMGR sync all IPSec SA to Flow started. 01/26 03:41:14
User admin logged in via Web from 192.168.6.56 using https 01/26 03:41:06
User 'admin' authenticated. From: 192.168.6.56. 01/26 03:41:06
Config installed 01/26 03:41:03
Dnsproxy object:mgmt-obj was enabled. 01/26 03:41:03
SSLMGR daemon configuration load phase-2 succeeded. 01/26 03:41:03
SATD daemon configuration load phase-2 01/26
Config Logs
Command Path Admin Time
commit admin 01/26 03:25:02
set deviceconfig system admin 01/26 03:22:22
delete deviceconfig system dns-setting dns-proxy-object admin 01/26 03:22:22
delete deviceconfig system dns-setting servers primary admin 01/26 03:22:08
delete deviceconfig system dns-setting admin 01/26 03:22:08
Locks
No locks found
ACC Risk Factor
No data found
System Resources
Management CPU 40%
Data Plane CPU 0%
Session Count 0 / 262142
admin | Logout
Tasks Language
12:39
2015-01-26


PA-3020
https://192.168.6.200/#device::vsys1::device/software
Szukaj
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Save
Help
29 items
Administrators
User Identification
VM Information Sources
High Availability
Certificate Management
Certificates
Certificate Profile
OCSP Responder
Response Pages
Log Settings
System
Config
HIP Match
Alarms
Manage Logs
Server Profiles
SNMP Trap
Syslog
Email
Netflow
RADIUS
LDAP
Kerberos
Local User Database
Users
User Groups
Authentication Profile
Authentication Sequence
Version | Size | Release Date | Downloaded | Currently Installed | Action
6.1.1 | 185 MB | 2014/12/18 03:48:26 | ✔ | | Install | Release Notes
6.1.0 | 391 MB | 2014/10/25 08:47:44 | ✔ | ✔ | Reinstall | Release Notes
6.0.8 | 253 MB | 2015/01/21 05:12:57 | ✔ | | Install | Release Notes
6.0.7 | 252 MB | 2014/12/08 22:02:40 | ✔ | | Install | Release Notes
6.0.6 | 252 MB | 2014/10/23 21:08:30 | | | Download | Release Notes
6.0.5 | 251 MB | 2014/09/23 11:19:58 | | | Download | Release Notes
6.0.5-h3 | 251 MB | 2014/10/08 16:40:41 | | | Download | Release Notes
6.0.4 | 229 MB | 2014/08/04 20:26:02 | | | Download | Release Notes
6.0.3 | 214 MB | 2014/06/12 00:16:54 | ✔ | | Install | Release Notes
6.0.2 | 208 MB | 2014/04/23 22:22:08 | | | Download | Release Notes
6.0.1 | 199 MB | 2014/03/09 11:12:01 | ✔ | | Install | Release Notes
6.0.0 | 410 MB | 2014/01/19 11:33:09 | ✔ | | Install | Release Notes
5.0.15 | 223 MB | 2014/11/20 04:54:05 | | | Download | Release Notes
5.0.14 | 219 MB | 2014/08/24 18:41:42 | | | Download | Release Notes
5.0.14-h3 | 222 MB | 2014/10/08 | | | Download | Release Notes
Check Now
Upload
Install From File
admin | Logout
Tasks
Language
12:39
2015-01-26

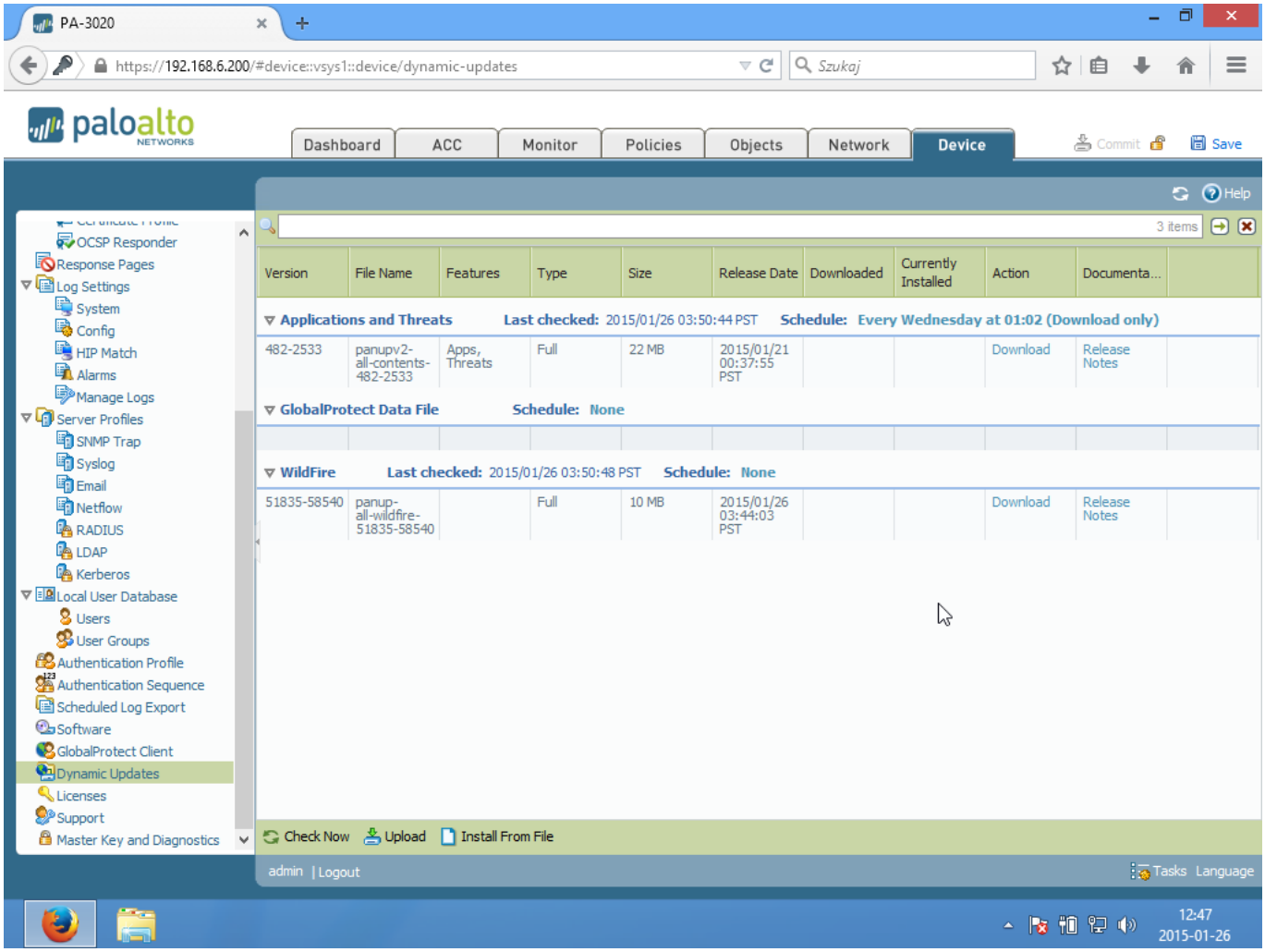


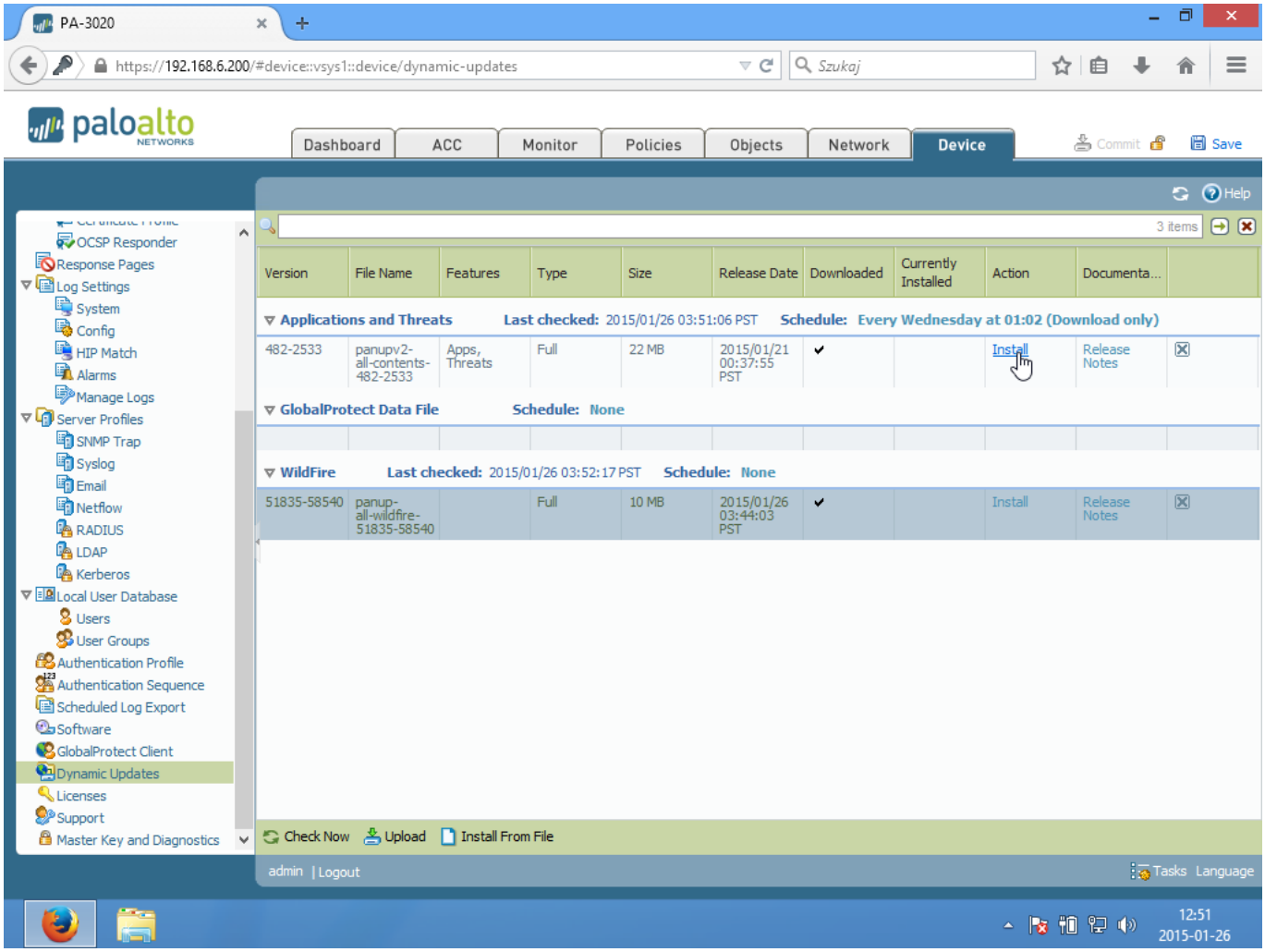
Już po chwili na naszym palo pojawia się najnowsza wersja 6.1.1.

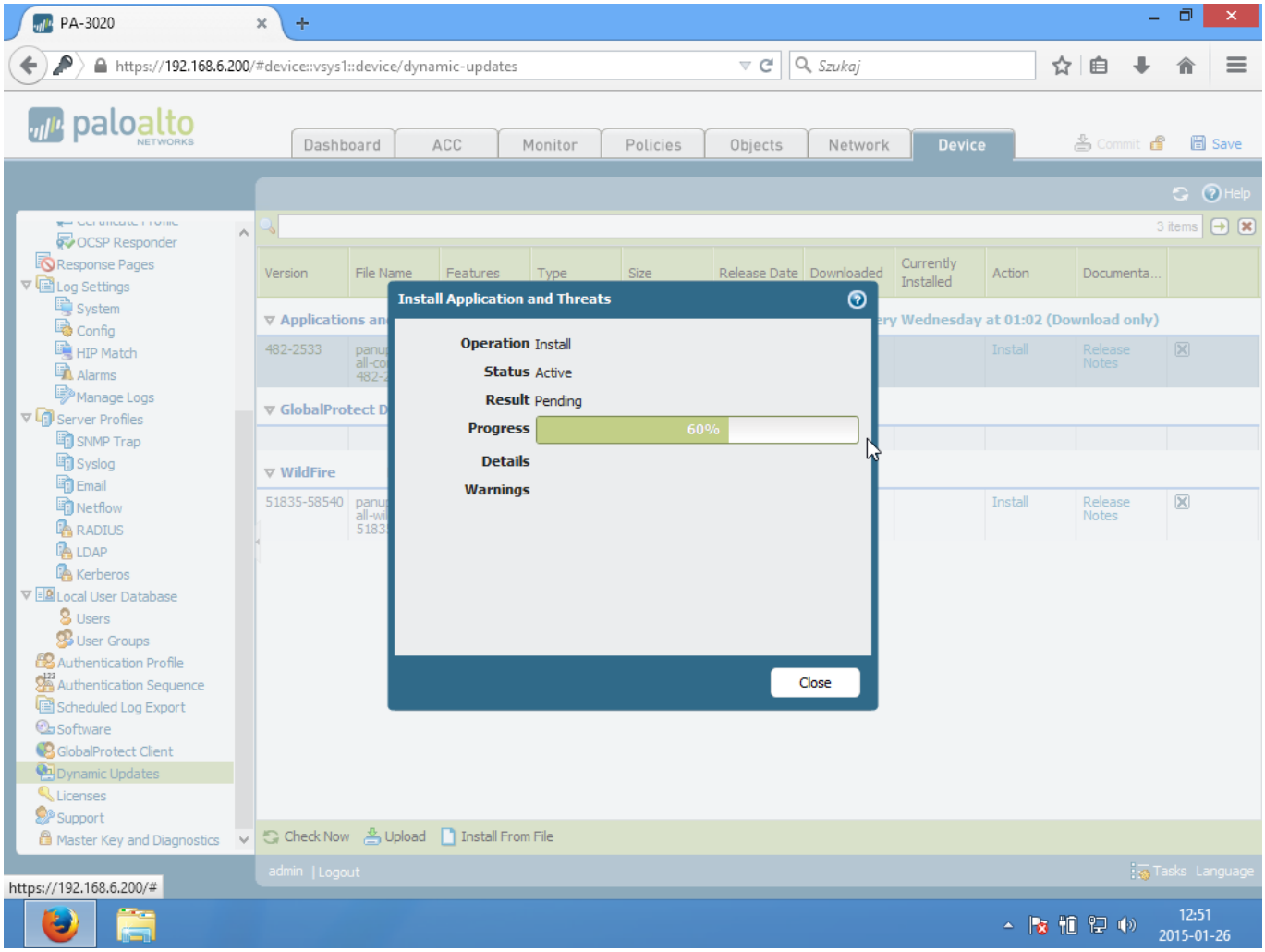


Następnym krokiem będzie aktualizacja sygnatur aplikacji. Aktualizacje wykonywane na bieżąco pozwalają nam na wczesne wykrywanie zagrożenia.

Tak jak w przypadku wersji systemu, najpierw należy pobrać aktualna listę aktualizacji. Następnie pobieramy aktualizacje i instalujemy.

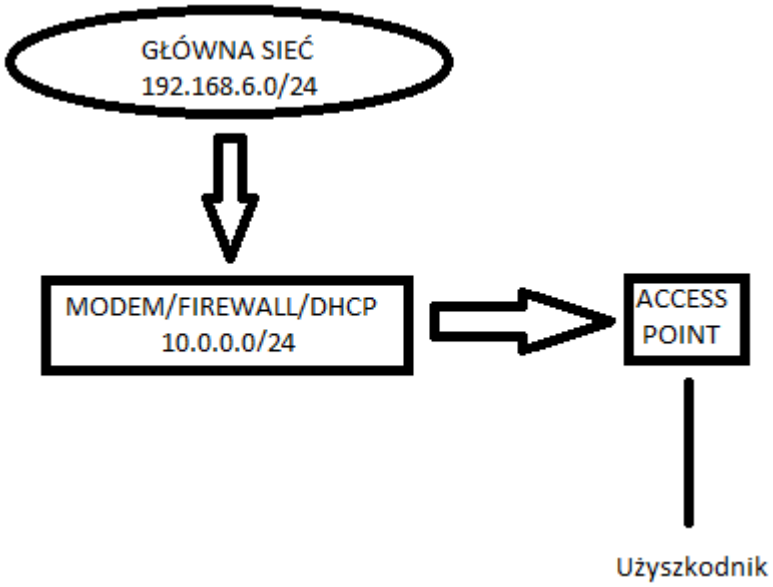

PA-3020
https://192.168.6.200/#device::vsys1::device/dynamic-updates
Szukaj
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Save
Help
3 items
OCSP Responder
Response Pages
Log Settings
System
Config
HIP Match
Alarms
Manage Logs
Server Profiles
SNMP Trap
Syslog
Email
Netflow
RADIUS
LDAP
Kerberos
Local User Database
Users
User Groups
Authentication Profile
Authentication Sequence
Scheduled Log Export
Software
GlobalProtect Client
Dynamic Updates
Licenses
Support
Master Key and Diagnostics
Version
File Name
Features
Type
Size
Release Date
Downloaded
Currently Installed
Action
Documenta...
Applications and Threats
Last checked: 2015/01/26 03:50:44 PST
Schedule: Every Wednesday at 01:02 (Download only)
482-2533
panupv2-all-contents-482-2533
Apps, Threats
Full
22 MB
2015/01/21 00:37:55 PST
Download
Release Notes
GlobalProtect Data File
Schedule: None
WildFire
Last checked: 2015/01/26 03:50:48 PST
Schedule: None
51835-58540
panup-all-wildfire-51835-58540
Full
10 MB
2015/01/26 03:44:03 PST
Download
Release Notes
Check Now
Upload
Install From File
admin | Logout
Tasks
Language
12:47
2015-01-26


PA-3020
https://192.168.6.200/#device::vsys1::device/dynamic-updates
Szukaj
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Save
Help
3 items
OCSP Responder
Response Pages
Log Settings
System
Config
HIP Match
Alarms
Manage Logs
Server Profiles
SNMP Trap
Syslog
Email
Netflow
RADIUS
LDAP
Kerberos
Local User Database
Users
User Groups
Authentication Profile
Authentication Sequence
Scheduled Log Export
Software
GlobalProtect Client
Dynamic Updates
Licenses
Support
Master Key and Diagnostics
Version
File Name
Features
Type
Size
Release Date
Downloaded
Currently Installed
Action
Documenta...
Applications and Threats
Last checked: 2015/01/26 03:51:06 PST
Schedule: Every Wednesday at 01:02 (Download only)
482-2533
panupv2-all-contents-482-2533
Apps, Threats
Full
22 MB
2015/01/21 00:37:55 PST
Install
Release Notes
GlobalProtect Data File
Schedule: None
WildFire
Last checked: 2015/01/26 03:52:17 PST
Schedule: None
51835-58540
panup-all-wildfire-51835-58540
Full
10 MB
2015/01/26 03:44:03 PST
Install
Release Notes
Check Now
Upload
Install From File
admin | Logout
Tasks
Language
12:51
2015-01-26



4. Sieć produkcyjna, przed wdrożeniem Palo Alto.

Kilka słów o sieci w której pracuje user. Jest ona prosta. Składa się z modemu/routera/firewalla oraz AP. User może łączyć się po wifi lub po kablu. Jako element stykowy użyto routera ON NETWORKS N300. Router ten, posiada możliwość rozgłaszania własnego wifi. My dziś z niego nie skorzystamy później wytłumaczę dlaczego. Dodatkowo w tym konkretnym scenariuszu został użyty router dlinka ustawiony w tryb Acces Point'a. Poniżej schemat sytuacyjny.



5. Blokowanie usług określonych w specyfikacji bezpieczeństwa korzystając ON NETWORKS N300.

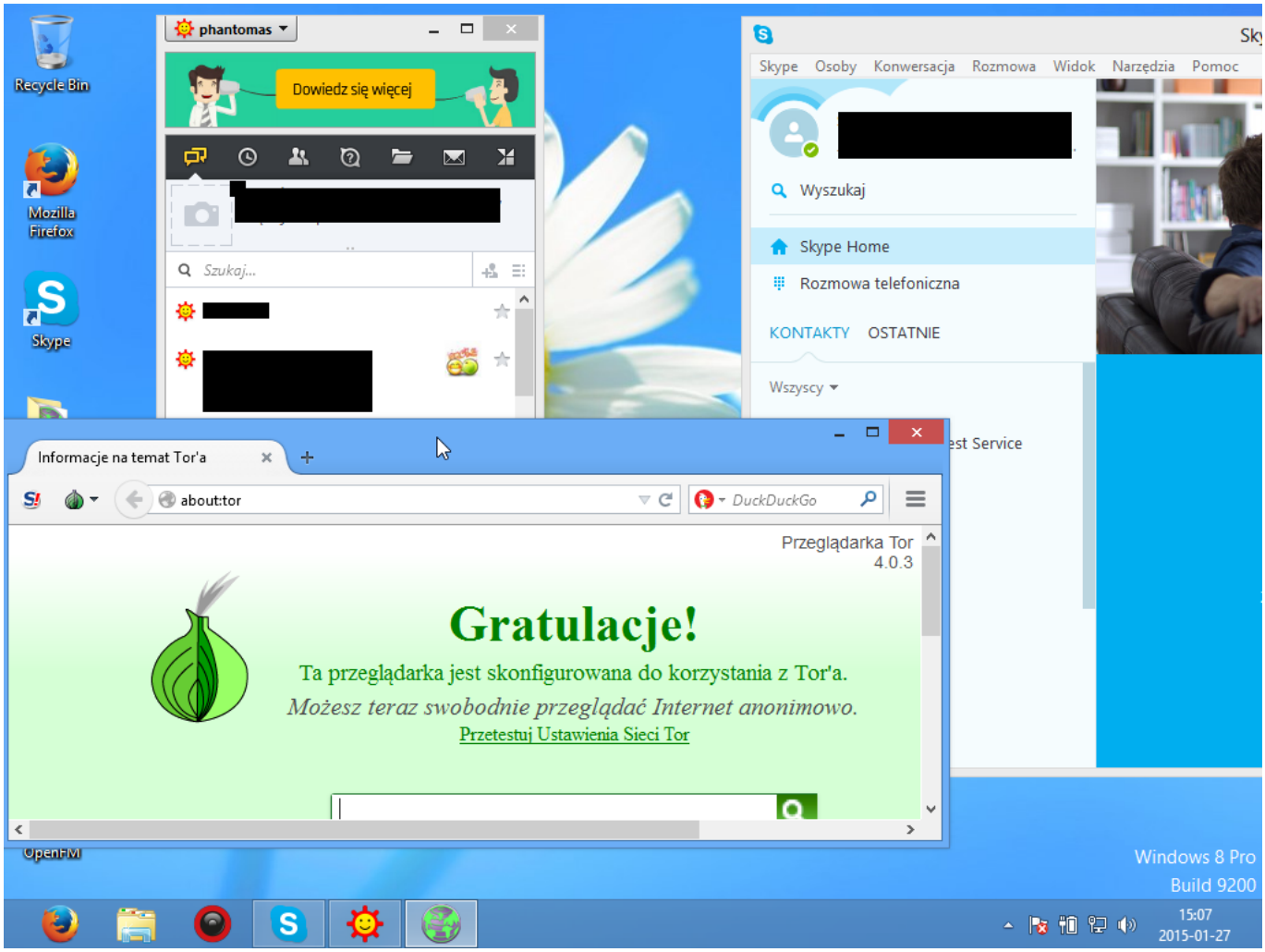
W założonej przez nas sytuacji, dział bezpieczeństwa it otrzymał wytyczne aby w sieci mu podlegającej zablokowane były konkretne usługi:

- Tor
- Ssh
- Gadu-Gadu
- Skype
- Facebook
- Gmail
- Transfer torentów
- VPN

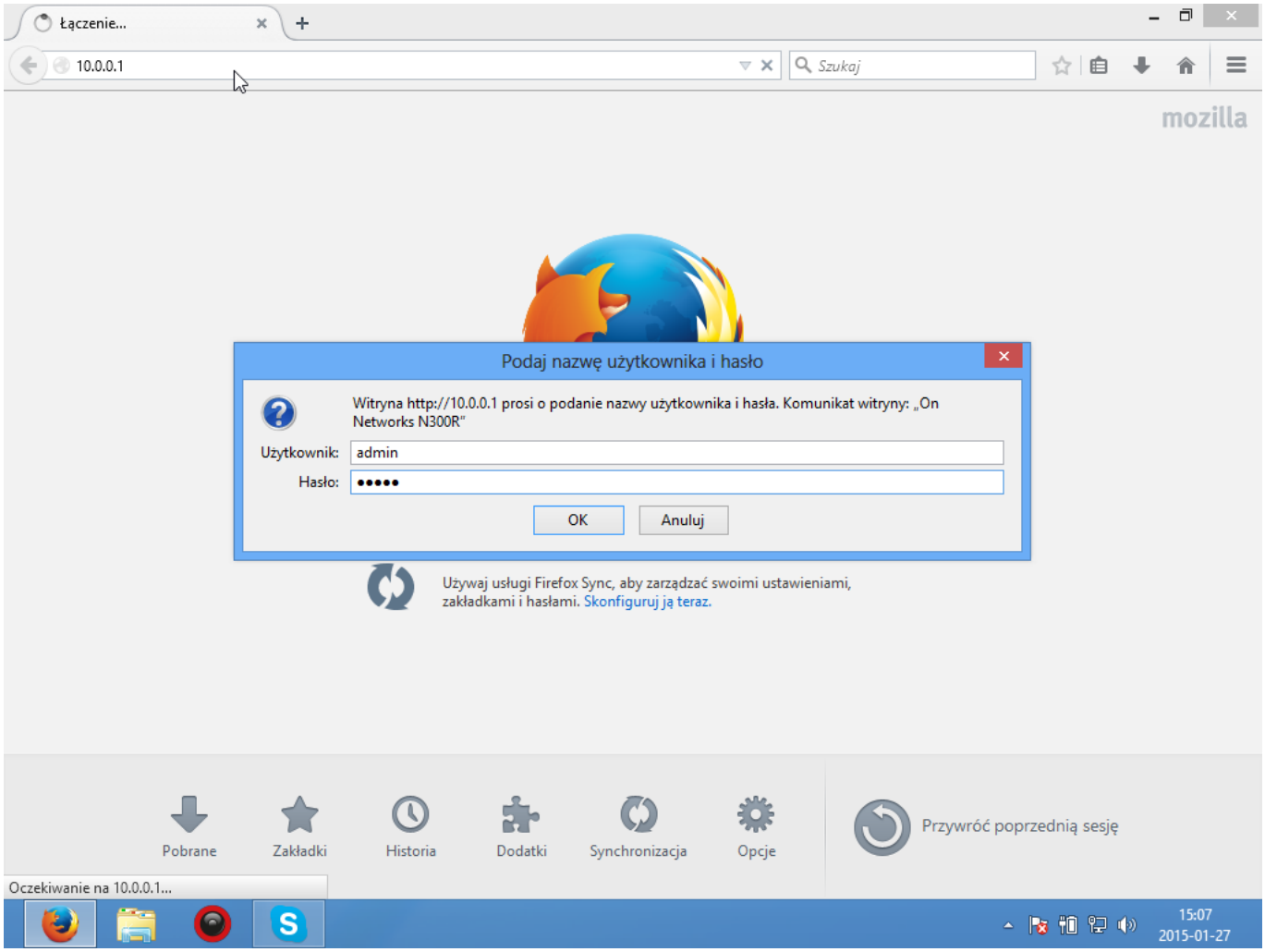
Dozwolone ma być korzystanie klientów pocztowych. Dalsze restrykcje maja być wprowadzane w miarę wykrywania nadużyć.

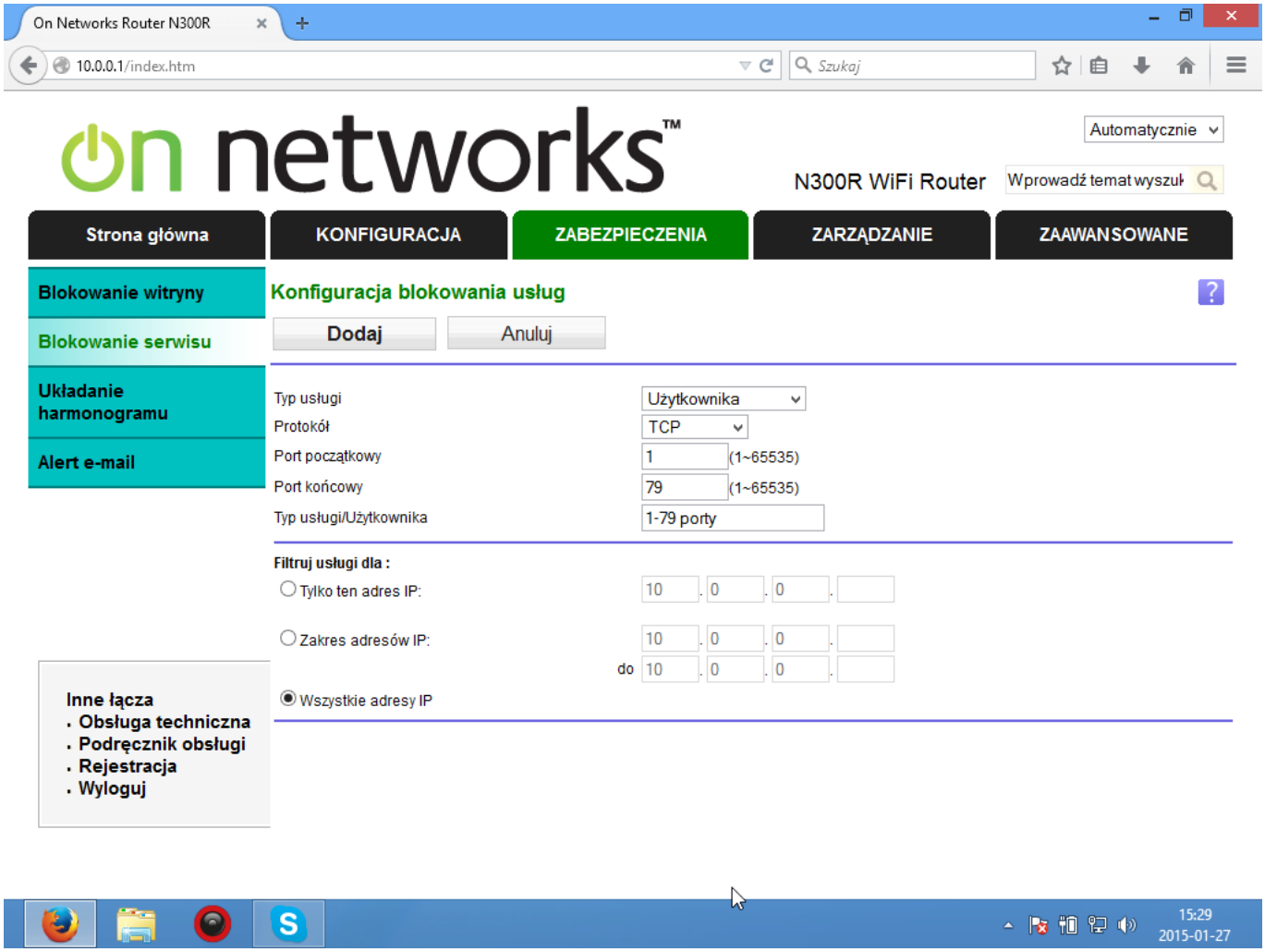
Blokowanie na standardowych firewallach odbywa się poprzez blokowanie IP/portu.

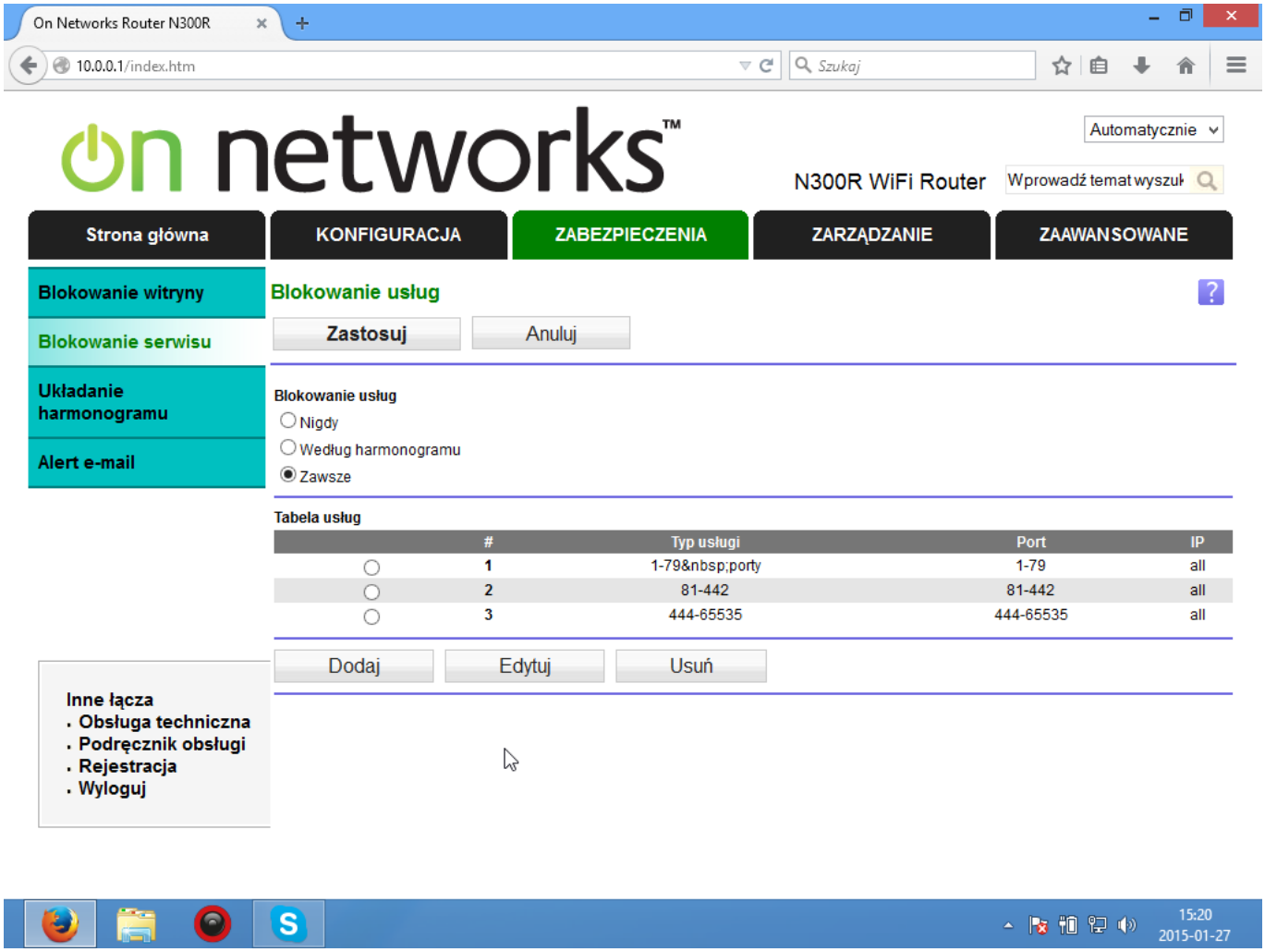
Poniżej przedstawiam widok pulpitu użytkownika przed wdrożeń restrykcji. Jak widzimy użytkownik lubi używać tora, Skype i GG zamiast pracować.



Czas zalogować się do naszego routera i zablokować usługi wymienione w specyfikacji.


Łączenie...
10.0.0.1
Szukaj
mozilla
Podaj nazwę użytkownika i hasło
Witryna http://10.0.0.1 prosi o podanie nazwy użytkownika i hasła. Komunikat witryny: „On Networks N300R"
Użytkownik:
admin
Hasło:
OK
Anuluj
Używaj usługi Firefox Sync, aby zarządzać swoimi ustawieniami, zakładkami i hasłami. Skonfiguruj ją teraz.
Pobrane
Zakładki
Historia
Dodatki
Synchronizacja
Opcje
Przywróć poprzednią sesję
Oczekiwanie na 10.0.0.1...
15:07
2015-01-27


On Networks Router N300R
10.0.0.1/index.htm
Szukaj
on networks™
Automatycznie
N300R WiFi Router
Wprowadź temat wyszuk
Strona główna
KONFIGURACJA
ZABEZPIECZENIA
ZARZĄDZANIE
ZAAWANSOWANE
Blokowanie witryny
Blokowanie serwisu
Układanie harmonogramu
Alert e-mail
Konfiguracja blokowania usług
Dodaj
Anuluj
Typ usługi
Użytkownika
Protokół
TCP
Port początkowy
1
(1~65535)
Port końcowy
79
(1~65535)
Typ usługi/Użytkownika
1-79 porty
Filtruj usługi dla :
Tylko ten adres IP:
Zakres adresów IP:
do
Wszystkie adresy IP
Inne łącza
Obsługa techniczna
Podręcznik obsługi
Rejestracja
Wyloguj
15:29
2015-01-27



Zablokowaliśmy wszystkie porty prócz 80 i 443. Można by rzec, że sukces. Spójrzmy do specyfikacji. Po chwili zastanowienia odkrywamy, że wycięliśmy przy okazji ruch klientów pocztowym. Gdybyśmy zrobili to na produkcji, w ciągu 10 minut pojawiła by się u nas pani z działy handlu, że nie może ofert wysłać, a przecież nie o to nam chodzi. Oczywiście można zmienić konfiguracje tak by wyciąć ruch poza klientami poczty. Ale! Właśnie, gdy zaczniemy działać w ten sposób:

- Musimy otworzyć ruch na 8 portach (80, 110, 143, 443, 465, 587, 993, 995). W ten sposób dajemy możliwość poruszania się tymi portami a więc zostawiamy dziurę w naszej „ścianie ognia".
- Z czasem może się okazać, że metoda „deny all, allow list" czyli zablokowanie wszystkiego prócz konkretnych portów spowoduje dużą ilość późniejszych rekonfiguracji.

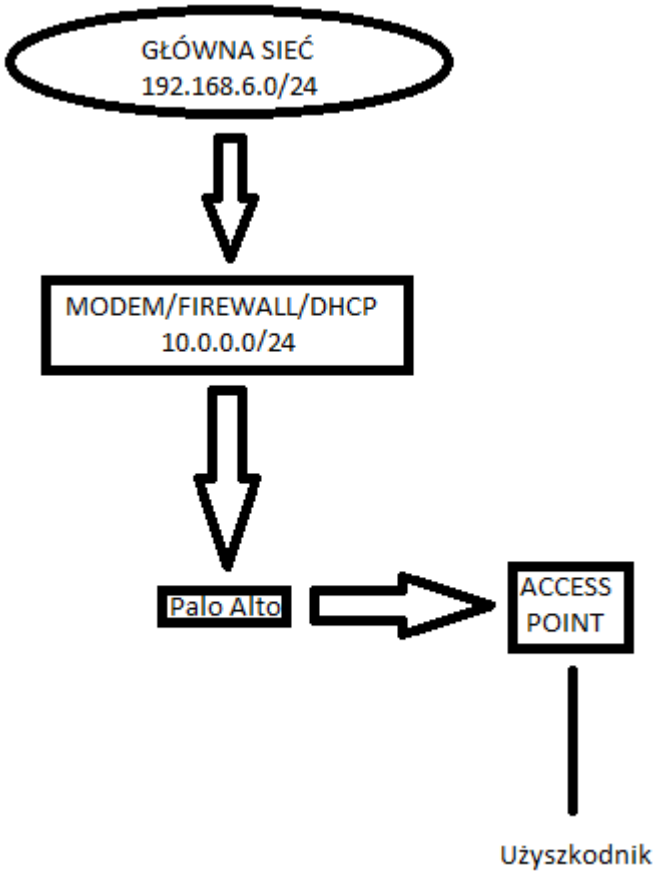
Zakładamy iż odblokowaliśmy klientów pocztowych i mamy zestaw wolnych portów: 80, 110, 143, 443, 465, 587, 993, 995.

Czy wiesz, że…. Aplikacje takie jak GG, Skype, Tor, Torenty posługują się dynamicznymi portami? To znaczy, że do momentu, gdy chociaż jeden port otwarty, tak długo będą one funkcjonować. Słabo prawda? VPN i SSH można dowolnie konfigurować tak by używały np portu 443 (bardzo popularna praktyka). Oczywiście nie mówię o Gmailu którego używamy za pomocą przeglądarki, która używa portów 80 i 443.

Co teraz? Czas na popis Palo Alto. Usuwamy wprowadzone zmiany i przechodzimy do wdrożenia next generation firewall.

6. Umieszczenie Palo Alto – Gdzie i dlaczego?

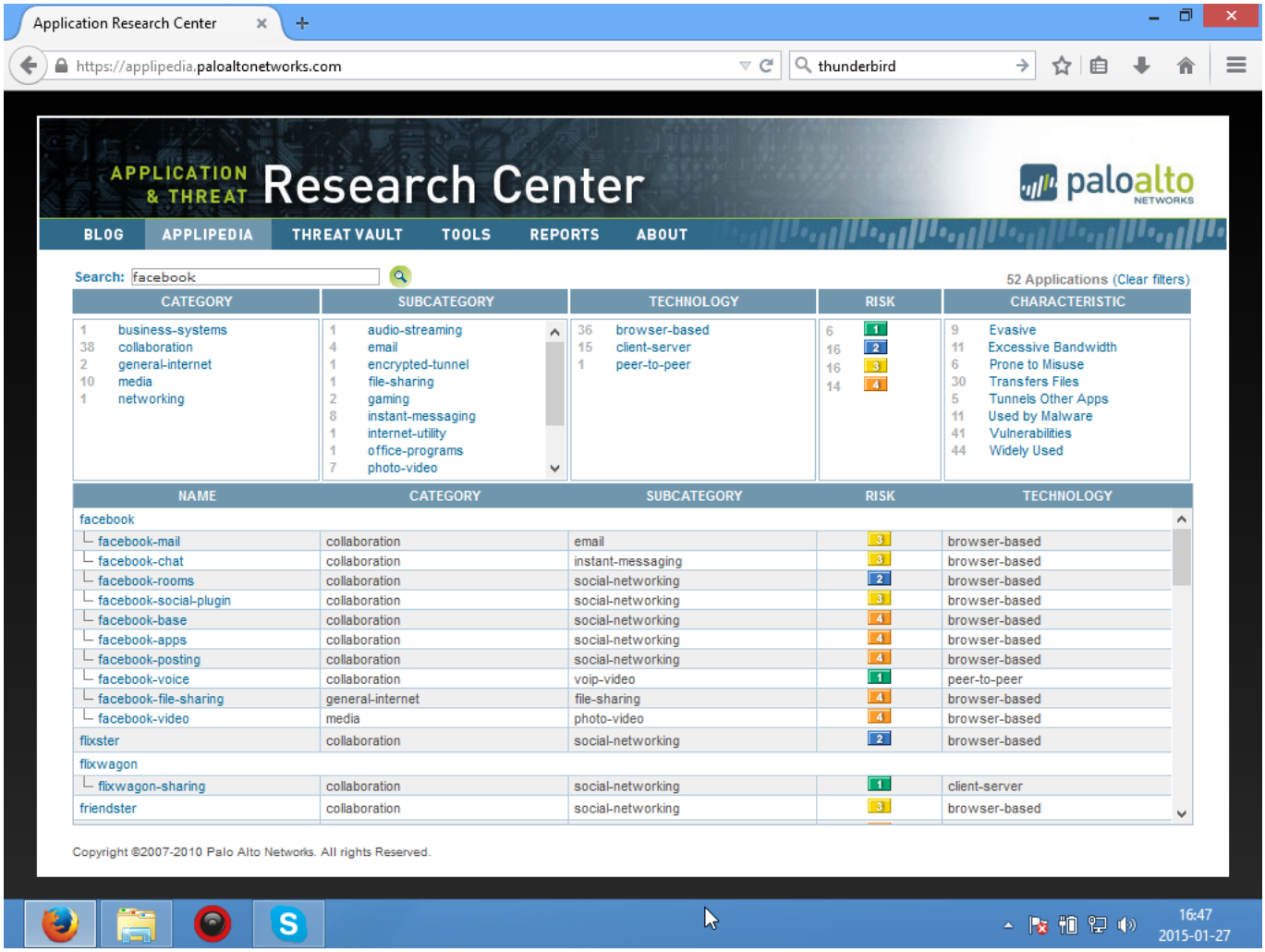
W momencie gdy postanawiamy wdrożyć Palo Alto, musimy zastanowić się gdzie chcemy je umieścić. Najlepszym rozwiązaniem będzie umieszczenie go na styku, zaraz za firewallem. Oto schemat:



W ten sposób przez palo będzie szedł cały ruch od użytkowników.

7. Wyszukiwanie w Aplipedii – Co blokować i jak?

Palo Alto udostępnia applipedie. Z niej dowiemy się co chcemy blokować.

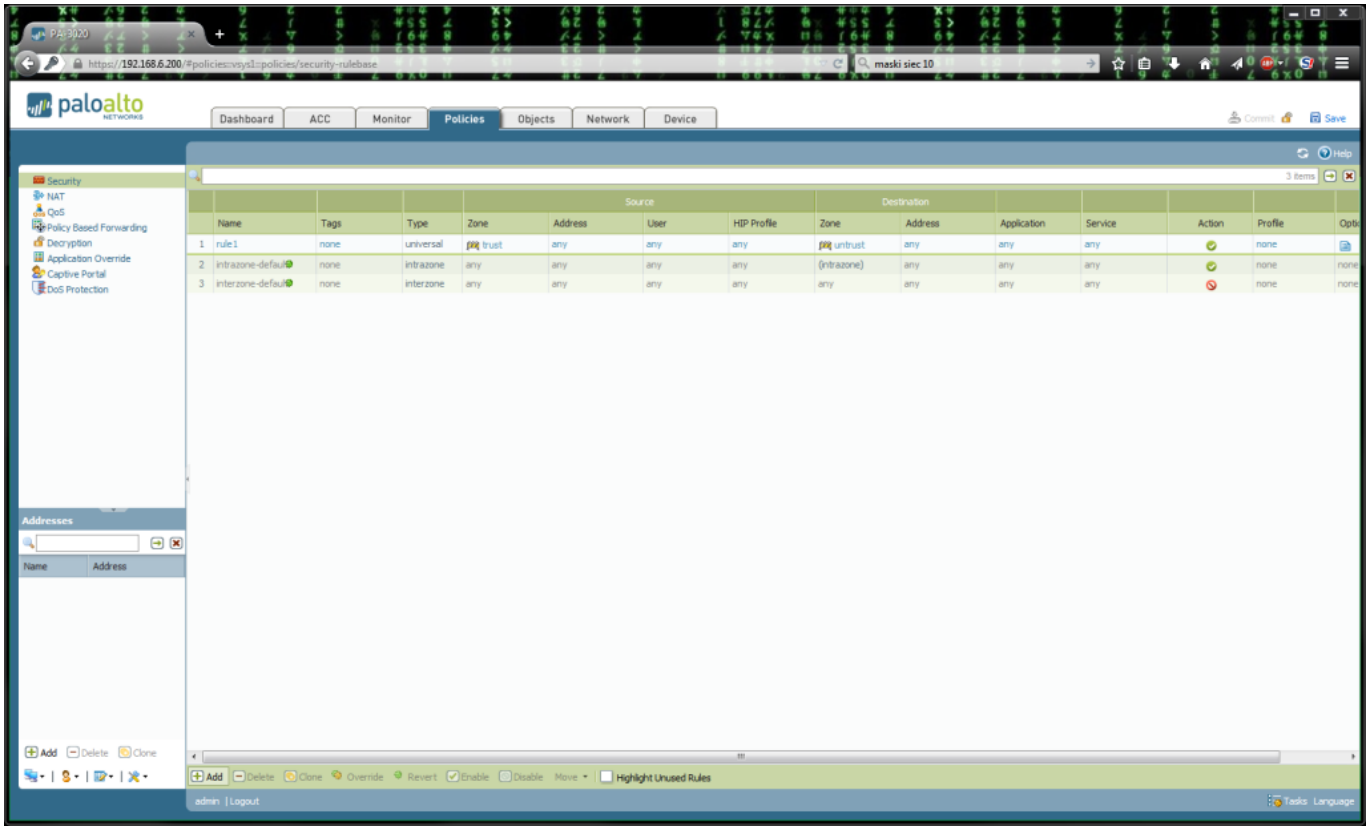


Robimy szybki rekonesans i dowiadujemy się, że Palo Alto pozwoli nam spełnić specyfikacje.

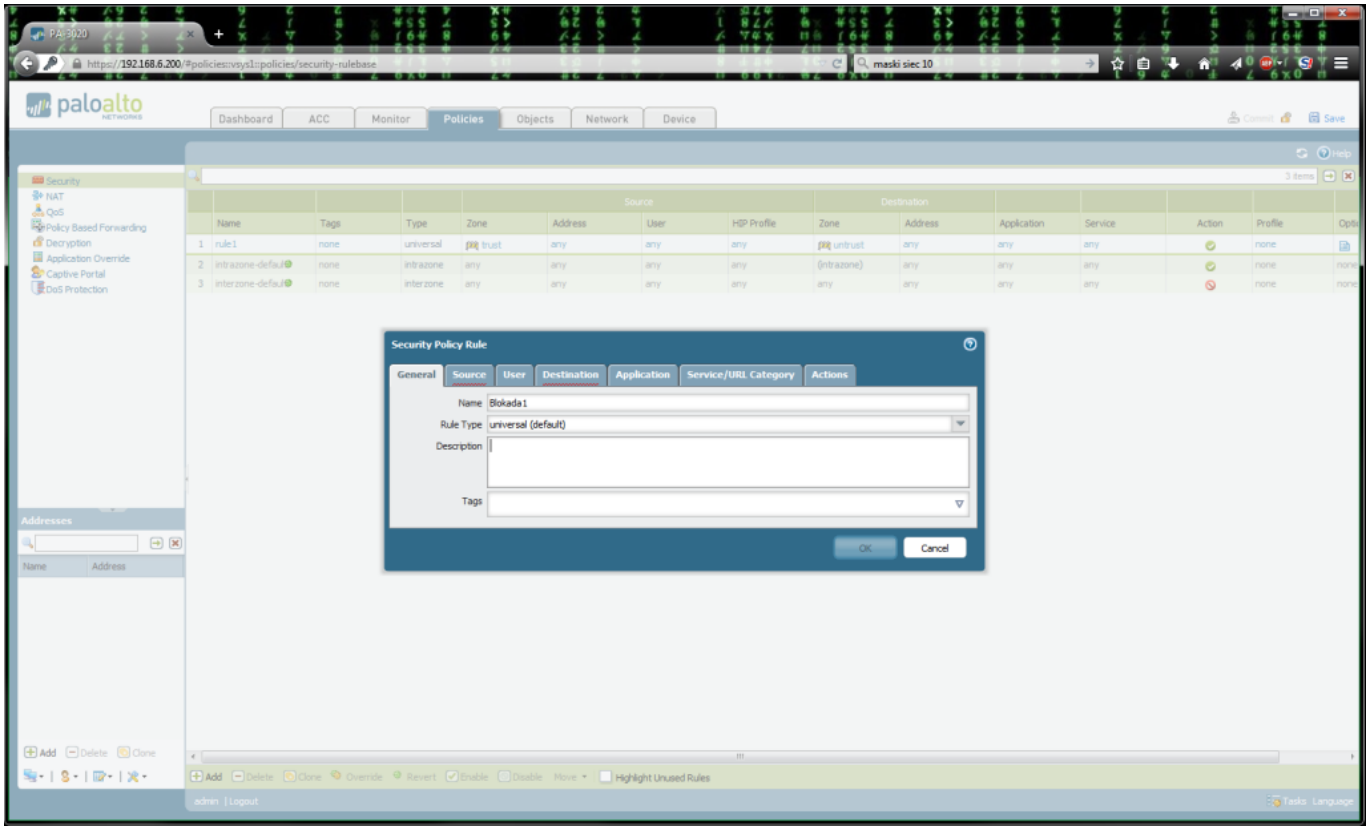
8. Wprowadzanie polityk bezpieczeństwa zgodnie z specyfikacja zadania.

Dochodzimy do sedna całego artykułu. Teraz dodamy do naszego nowego firewall'a nowe polityki bezpieczeństwa blokujące wymienione w specyfikacji usługi.

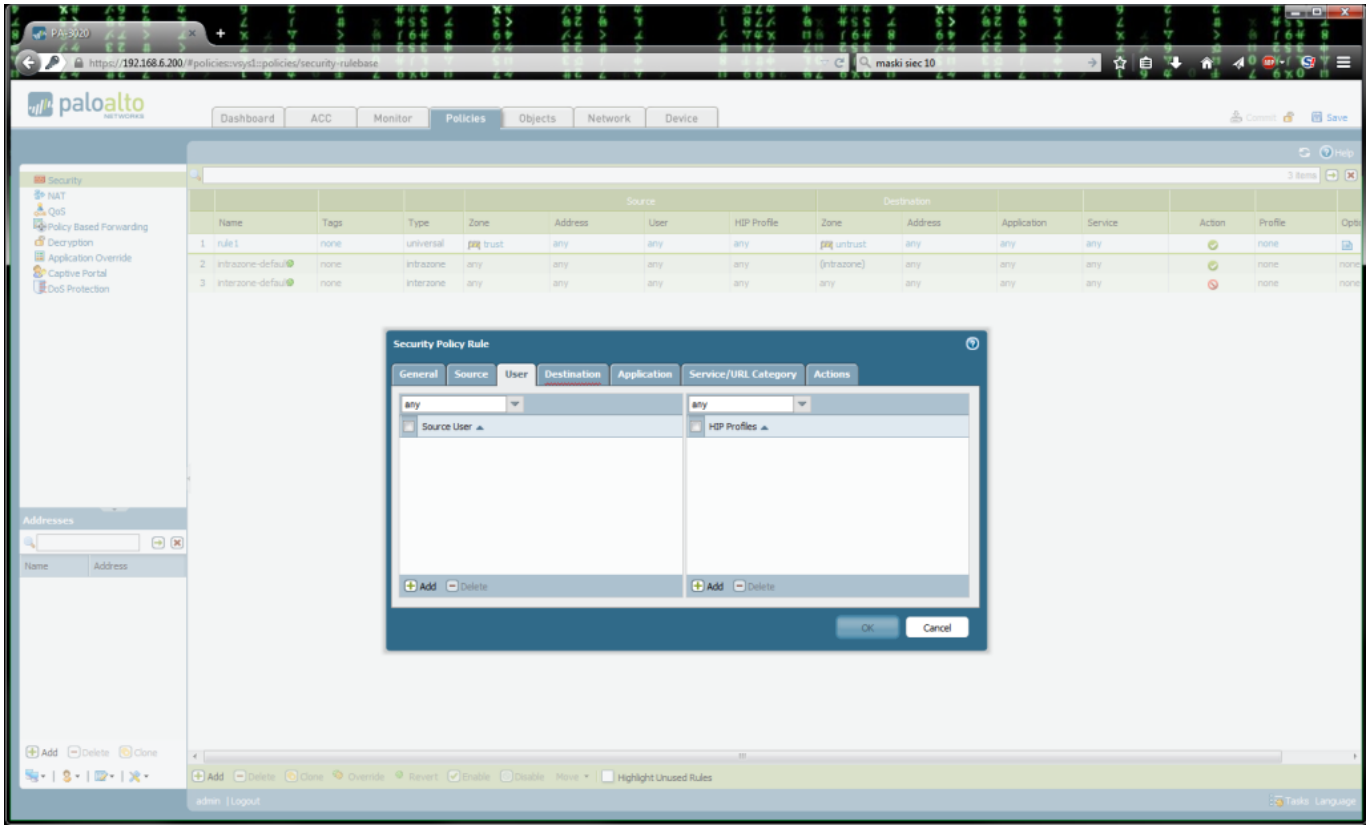
Logujemy się do naszego palo alto, przechodzimy do zakładki „Policies". W tej zakładce wylistowane są polityki bezpieczeństwa



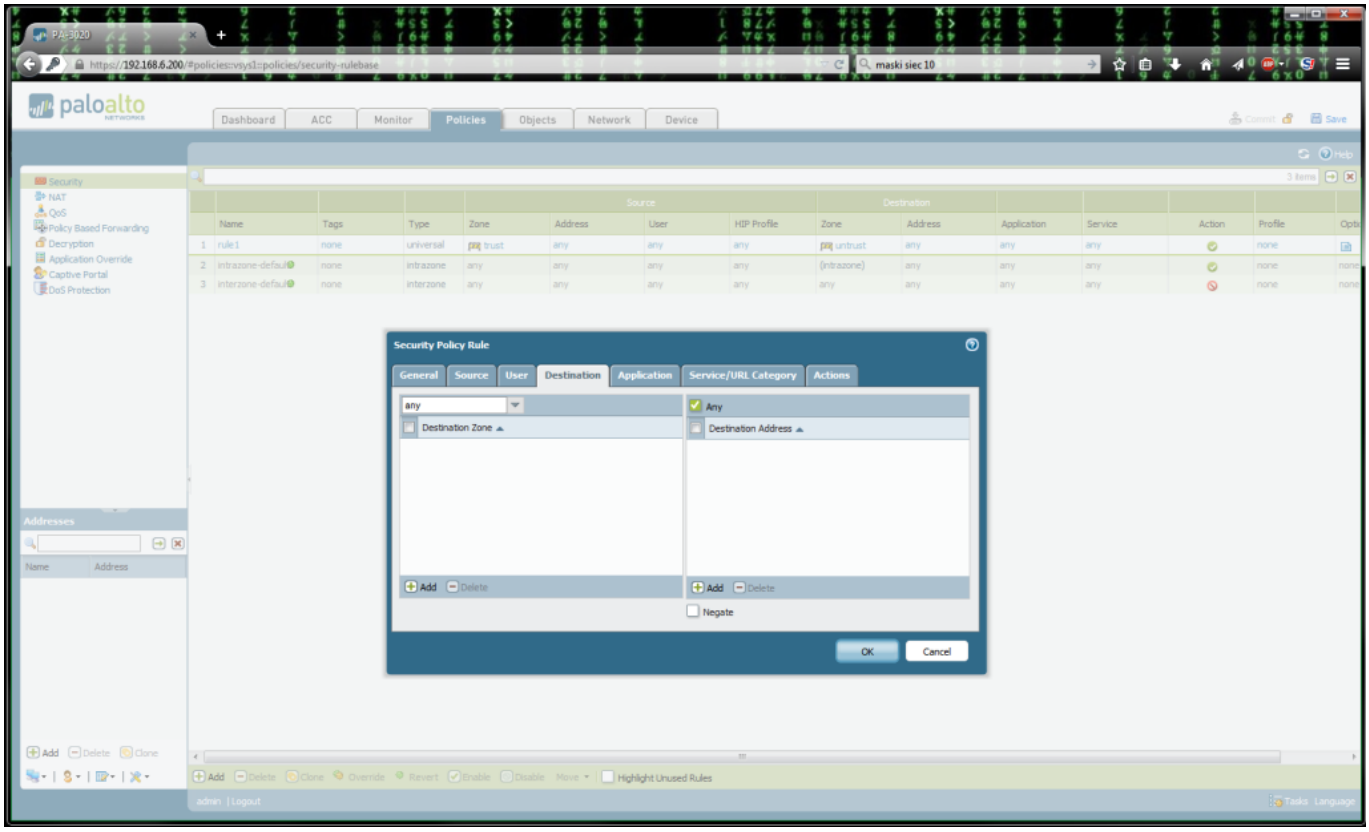
Aby dodać nową politykę klikamy „Add". Uzupełniamy pole „Name".



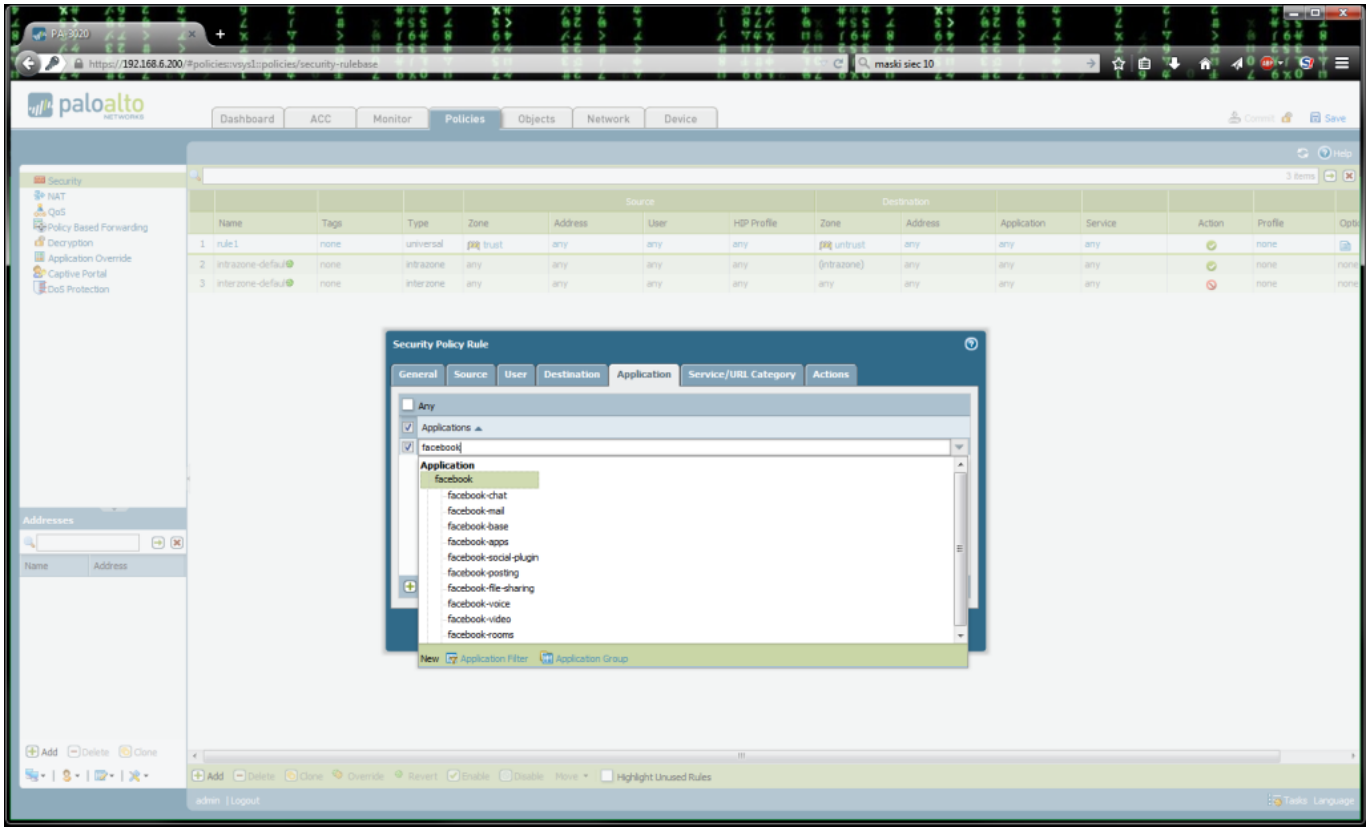
Pierwsza nowość, której niema w zwykłych firewallach. Zakładka user, to zakładka w której możemy spiąć nasze firmowe AD z palo i wybierać konkretnie per user jaki ruch ma być puszczany. Zostawiamy puste, nie mamy AD w specyfikacji.



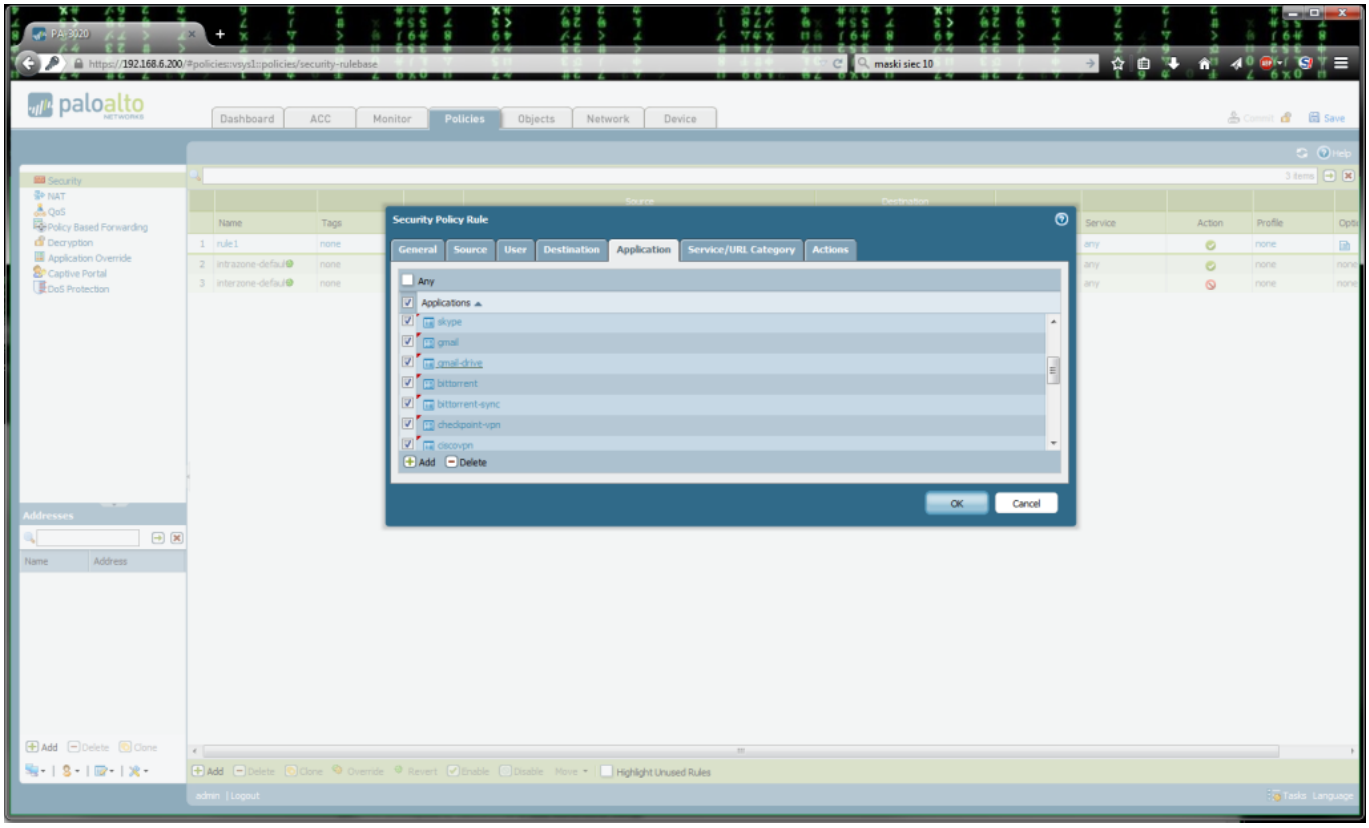
W zakładce „Destination" ustalamy kierunek ruchu. Obecnie mamy dwie strefy, „Trust: i „untrust" gdzie trust to nasza lokalna a untrust to internet. Możemy ustawić na trust (czyli na ruch wychodzący). Jednakże jeżeli wystawiamy jakieś porty na zewnątrz, warto jest dać „any".



W zakładce „Application" określamy jakie aplikacje maja być blokowane. Aplikacje? Przecież to niemożliwe! A jednak. Jak juz pisałem palo alto to next generation firewall działający na L7 a wiec na warstwie aplikacyjnej.



Korzystając z wyszukiwarki dodajemy kolejna aplikacje

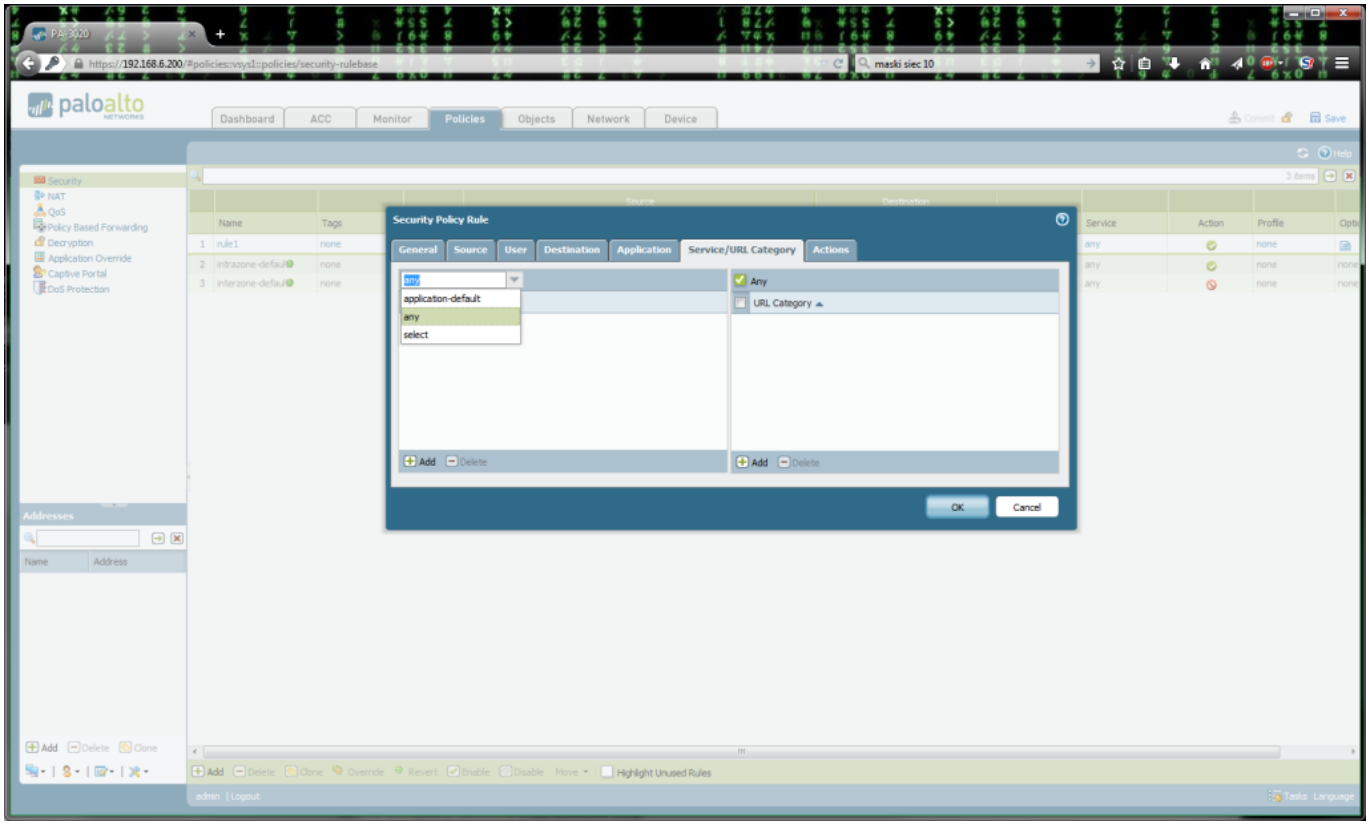


Pełna lista zablokowanych prze zemnie aplikacji:

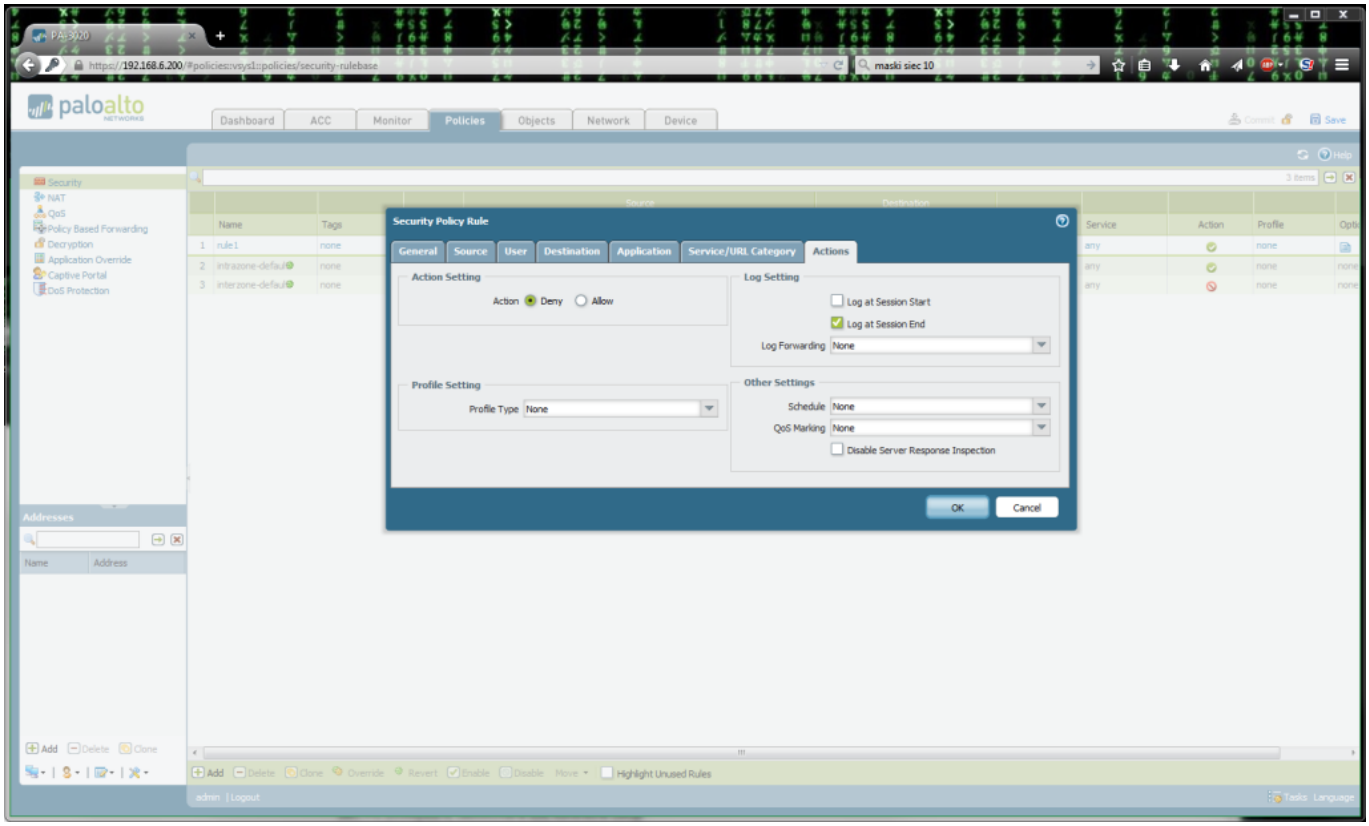
- bittorrent
- bittorrent-sync
- checkpoint-vpn
- ciscovpn
- cyberghost-vpn
- droidvpn
- facebook
- gadu-gadu
- gmail
- gmail-drive
- kerio-vpn
- open-vpn
- packetix-vpn
- skype
- ssh
- ssh-tunnel

- steganos-vpn
- tinyvpn
- tor
- vipnet-vpn
- wallcooler-vpn

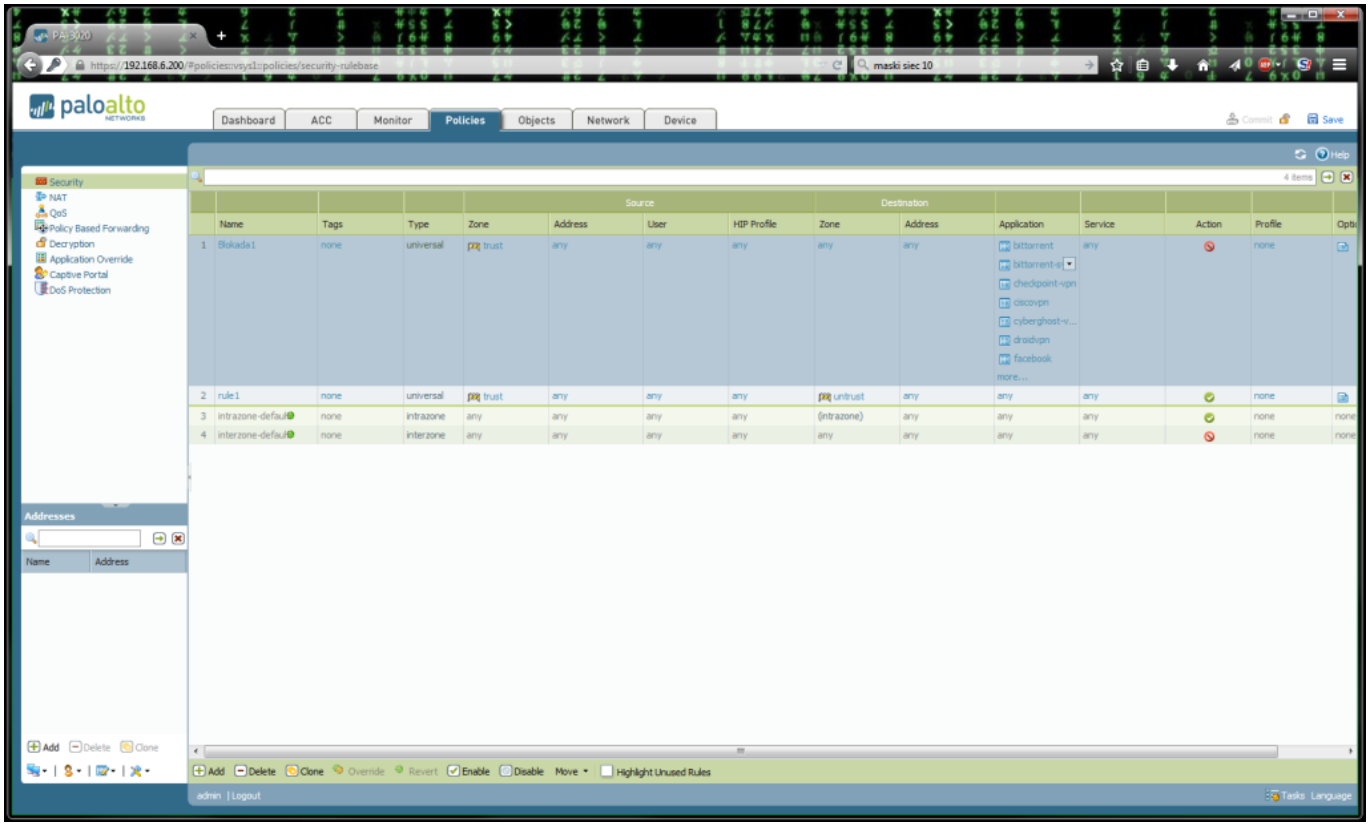
Zakładka „Service/Url Category" To tutaj wybieramy co dokładnie ma być brane pod uwagę. Czy typowe dla aplikacji porty i linki, czy wszystkie gdzie zostanie wykryty protokół danej aplikacji.



Zakładka „Actions" to tutaj podejmujemy decyzje – blokujemy czy pozwalamy na ruch.

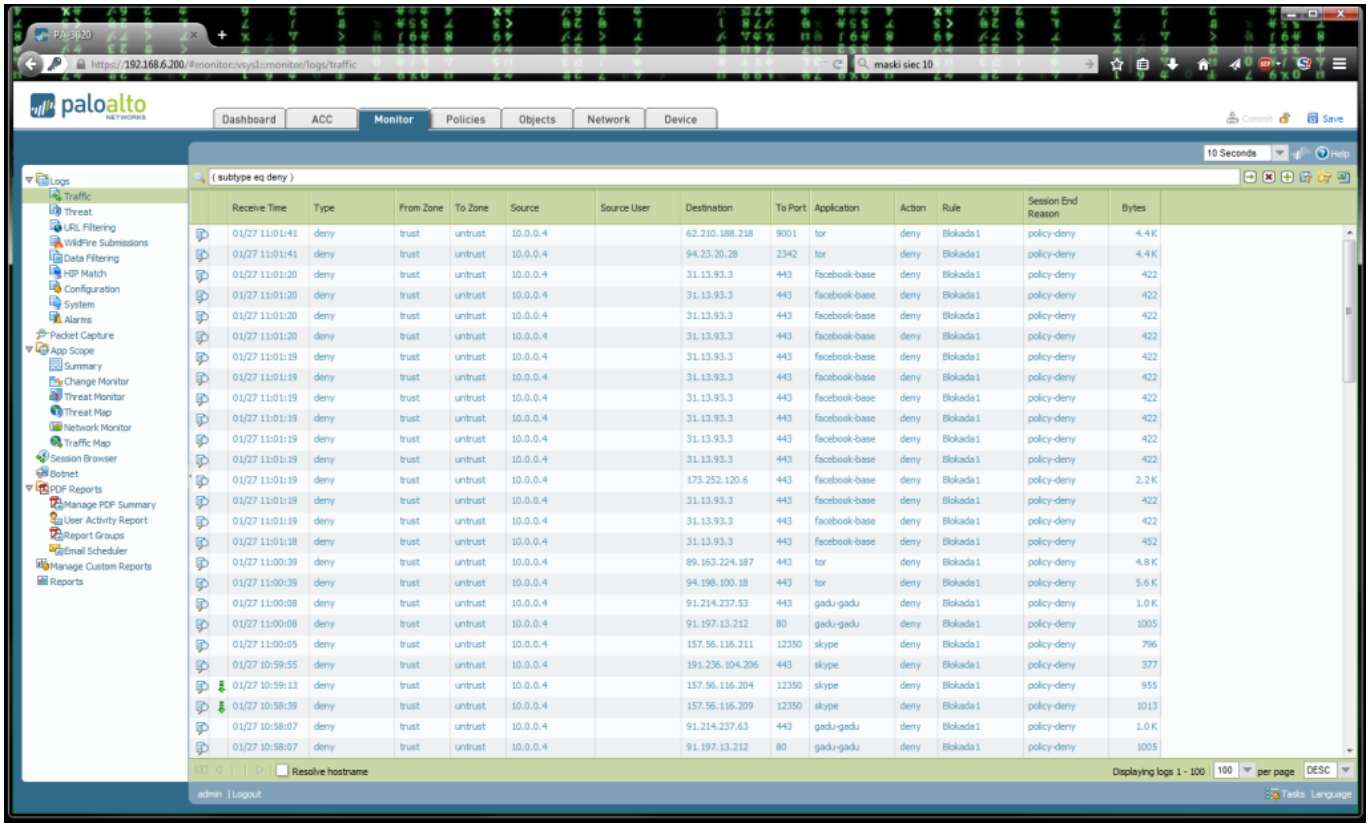


Poniżej widać dodana regułkę. Oczywiście następnie klikamy „Commit" aby zatwierdzić zmiany.



Po zatwierdzeniu zmian, przechodzimy do zakładki „Monitor", aby zaobserwować zmiany.

9. Obserwacja efektów wprowadzenia restrykcji zgodnych z specyfikacja bezpieczeństwa.



Po uruchomieniu odpowiedniego filtra widzimy ruch generowany przez użytkownika. Widać, iż osobnik ten generuje ruch z aplikacji tor, GG, Skype i Facebook. Zgodnie z ta specyfikacją ruch ten jest blokowany. Dzieje się tak, ponieważ nasz firewall blokuje ruch na danym porcie, ale przede wszystkim rozszywa ruch i identyfikuje rodzaj pakietów które przez niego przechodzą.

10. Odtworzenie sytuacji z posta, w której wycięty jest tor i omówimy ewentualne metody ominięcia zabezpieczenia w celu dostania się do sieci TOR.

W wcześniej przytoczonym prze zemnie poście z forum, mamy kilka informacji oto one:

- W sieci jest Cisco, zapewne ISE.
- W sieci jest Next Generation Firewall – Fortigate

Długo zastanawiałem się czy na pewno jest to Fortigate a nie na przykład po prostu Cisco ASA, ale postanowiłem zaufać postowi. W poście mamy jeszcze informacje, że cały problem

leży w tym że nie możliwym jest nawiązanie połączenia z siecią tor. Log który został tam zaprezentowany mówi jedynie, że połączenie nie może zostać nawiązane

Bazując na informacjach z posta w najbardziej optymistycznej opcji należy sprawdzić czy blokowany jest ruch:

- ssh
- vpn

Jeżeli któryś z powyższych nie jest blokowane należy wykorzystać to do tunelowania do maszyny która ma podpięty tor do interfejsu sieciowego. W przypadku vpn, jest to o tyle proste, że należy zainstalować tora oraz serwer vpn na zewnętrznej maszynie. Następnie zestawić połączenie tunelem do tej maszyny. Będziemy wtedy wychodzić z maszyny lokalnej do serwera vpn który będzie kierował ruch do sieci tor.

Można również użyć opcji tunelowania za pomocą ssh, ale odradzam, ponieważ zgodnie moją wiedzą, zostanie to szybko wykryte i zablokowane. Należy pamiętać, aby podczas działania nie zwracać na siebie uwagi. Oprócz blokowania możemy zostać oskarżeni o naruszenia regulaminu sieci i zostać ukarani.

11. Zapobieganie naruszeniom wymienionym w punkcie 10.

Zapobieganie naruszeniom jest obszernym tematem. Jak wcześniej wykazałem, z pomocą Next Generation Firewall jest to proste. Ważnym jest, aby podczas projektowania polityk bezpieczeństwa kierować się nie tylko ryzykiem, ale zakładać, iż użytkownik jest w stanie obejść nasze zabezpieczenie i blokować niepotrzebne usługi tak jak ja to zrobiłem. Blokując TOR należy zablokować vpn i ssh. Gdzie mówiąc o blokowaniu nie mam na myśli blokowaniu portów a blokowanie protokołu. Dodatkowym sposobem jest regularne sprawdzanie logów w celu identyfikacji zagrożeń i dostosowania polityk bezpieczeństwa.