FIREWALLE: PRZEWODNIK DLA KLIENTÓW

Praktyczny przewodnik dobierania firewalli dla sieci w przedsiębiorstwach.

paloalto NETWORKS®

the network security company™

Zmiany, rozwiązania, innowacje

Nawet firewalle z bardziej zaawansowanymi funkcjami i wydajnością większą niż dotychczas przechodzą „kryzys tożsamości". Zagrożenia szybko ewoluują, a tradycyjne filtrowanie portów i adresów IP nie zapewnia już odpowiedniej ochrony.

Wprowadzenie

Bez wątpienia sieci są obecnie bardziej złożone niż dotychczas. Pracownicy uzyskują dostęp do dowolnej aplikacji przy użyciu urządzeń służbowych lub osobistych. W wielu wypadkach są to aplikacje przeznaczone do użytku zarówno osobistego, jak i służbowego, jednak ryzyko biznesowe i zabezpieczenia są często ignorowane. Nowi potencjalni pracownicy pytają o zasady korzystania z aplikacji przed zaakceptowaniem nowej posady. Dodanie kolejnej warstwy złożoności jest ważnym problemem związanym z efektywnością systemu zabezpieczeń elektronicznych. Czy firma jest celem ataków? Czy chodzi raczej o to „kiedy", a nie o to „czy"? Czy można lepiej się przygotować? Złożoność sieci oraz infrastruktury zabezpieczeń może ograniczać zdolność do szybkiego reagowania na te i inne wyzwania związane z bezpieczeństwem w cyberprzestrzeni.

Gdy większa złożoność sieci ogranicza możliwość szybkiego podejmowania optymalnych decyzji, zazwyczaj pomocne jest „skoncentrowanie się na podstawach" w celu rozwiązania bieżących problemów technicznych w najbardziej efektywny sposób. W ten sposób przypominamy sobie o trzech podstawowych funkcjach firewalla:

1. Pełnienie funkcji podstawowego składnika infrastruktury zabezpieczeń sieci.

2. Pełnienie funkcji punktu kontroli dostępu dla całego ruchu sieciowego (akceptowanie lub odrzucanie ruchu skierowanego do sieci na podstawie zasad).

3. Eliminacja ryzyka związanego z „nieznanymi" zagrożeniami przy użyciu pozytywnego modelu kontroli, zgodnie z którym należy zezwalać na dowolny ruch sieciowy, jednak domyślnie blokować cały pozostały ruch.

Z upływem czasu podstawowe funkcje firewalla zostały wyeliminowane właśnie z powodu kontrolowanego przez nią ruchu sieciowego. Rozwój aplikacji spowodował, że podstawowa infrastruktura zabezpieczeń nie zapewnia już poziomu kontroli wymaganego do ochrony cyfrowych zasobów użytkowników.

Wymiana portów (port hopping), korzystanie z niestandardowych portów i użycie szyfrowania to przykłady metod ułatwiających dostęp do aplikacji. Te same techniki są używane również przez osoby atakujące firmy w cyberprzestrzeni zarówno bezpośrednio (cyberzagrożenia stwarzane przez te osoby), jak i pośrednio (ukrywanie zagrożeń w ruchu sieciowym związanym z aplikacją). Problemy wprowadzane przez te nowoczesne aplikacje dodatkowo komplikuje fakt, że pracownicy używają ich do wykonywania zadań służbowych. W sieci występują między innymi następujące aplikacje i zagrożenia:

- **Typowe aplikacje użytkowników końcowych:** Przykłady aplikacji to multimedia społecznościowe, udostępnianie plików, wideo, wiadomości błyskawiczne i poczta elektroniczna. Stanowią one około 25% aplikacji w sieci i wykorzystują 20% przepustowości[1]. Niektórzy pracownicy mogą używać ich do celów związanych z obowiązkami służbowymi, a inni wyłącznie do użytku osobistego. Aplikacje te mogą być bardzo rozbudowane i często oferują funkcje związane z nieuzasadnionym ryzykiem. Są one związane zarówno z ryzykiem biznesowym, jak i zagrożeniem dla systemu zabezpieczeń i konieczne jest optymalne skonfigurowanie zezwalania na niektóre aplikacje i blokowania innych.

- **Podstawowe aplikacje biznesowe:** Te aplikacje są używane do prowadzenia działalności biznesowej i obsługują najważniejsze zasoby (np. bazy danych, usługi udostępniania plików i drukowania, katalogi). Ta grupa aplikacji jest obiektem ataków w cyberprzestrzeni, związanych z wieloma aspektami aplikacji, a podstawowym problemem jest najlepsze izolowanie i zabezpieczenie ich przed atakami w trybie niewidzialności, ułatwiającym pokonanie firewalla i systemu IPS przy użyciu typowych metod obchodzenia zabezpieczeń.

- **Aplikacje niestandardowe i związane z infrastrukturą:** Do tej grupy należą podstawowe aplikacje infrastruktury (np. SSL, SSH i DNS) i aplikacje opracowane wewnątrz organizacji, niestandardowe lub nieznane. Te aplikacje są powszechnie używane do maskowania poleceń i ruchu sterującego generowanego przez złośliwe oprogramowanie (np. roboty). Wiele z tych aplikacji korzysta z różnych niestandardowych portów. Osiemdziesiąt pięć z 356 aplikacji używających SSL nigdy nie korzysta z portu 443 ani portów zdefiniowanych dla protokołu SSL (37 stosuje metodę wymiany portów „port hopping", 28 używa portu tcp/80, a 20 korzysta z portów innych niż tcp/443).

[1] Raport dotyczący użycia aplikacji i zagrożeń Palo Alto Networks, styczeń 2013

Aby rozwiązać te problemy, zwrócono większą uwagę na podstawy firewalli, a każdy dostawca firewalli ponownie rozważa metody identyfikowania i kontrolowania ruchu na podstawie aplikacji, a nie tylko portu i protokołu. Firewalle kontrolujące ruch na podstawie aplikacji są obecnie zbiorczo zwane „firewallami nowej generacji", a każdy dostawca firewalla przyznaje, że kontrolowanie aplikacji jest obecnie jednym z najważniejszych aspektów zabezpieczeń sieci.

Istnieją dwie oczywiste przyczyny tego koncentrowania się na podstawach. Po pierwsze aplikacje i skojarzone zagrożenia mogą w łatwy sposób omijać firewalle blokujące porty i dodatkowe zabezpieczenia. Po drugie firewall jest jedyną lokalizacją, w której są dostępne wszystkie informacje dotyczące ruchu sieciowego i w której można efektywnie egzekwować zasady kontroli dostępu. Zalety tego nowego rozwiązania są oczywiste: skuteczność zabezpieczeń powinna być większa, a ilość zasobów administracyjnych wymaganych do zarządzania firewallem i reagowania na wypadki naruszenia systemu zabezpieczeń powinna być mniejsza lub co najmniej stała.

Rewolucja, nie ewolucja
Ze względu na zbyt duże natężenie ruchu sieciowego, nadmierną liczbę aplikacji i niedostateczną tolerancję na negatywny wpływ na wydajność nie można wciąż dodawać urządzeń i nowych „modułów" oprogramowania w celu ułatwienia analizy ruchu.

Definicja firewalli nowej generacji

Firewalle nowej generacji są definiowane przez firmę Gartner jako nowe rozwiązanie dla przedsiębiorstw „uwzględniające pełną inspekcję stosu umożliwiającą zapobieganie intruzjom, inspekcję na poziomie aplikacji i precyzyjną kontrolę przy użyciu zasad". Większość dostawców zabezpieczeń sieci zapewnia obecnie widoczność i kontrolę aplikacji przy użyciu sygnatur aplikacji dodawanych do silnika IPS lub oferuje dodatkową licencję na moduł kontroli aplikacji. Obie te opcje są dodatkami do firewalla blokującego porty i w niewielkim stopniu ułatwiają koncentrowanie się na podstawowych zadaniach, które powinien wykonywać firewall.

Efektywność funkcjonowania firmy jest w dużym stopniu zależna od aplikacji używanych przez pracowników i zawartości obsługiwanej przez te aplikacje. Ograniczenie się do blokowania tylko wybranych składników może spowodować zmniejszenie wydajności w firmie. Jeżeli zespół ds. zabezpieczeń poszukuje funkcji dostępnych w firewallach nowej generacji, należy w pierwszej kolejności ustalić, czy dany firewall nowej generacji umożliwi bezpieczne użytkowanie aplikacji z korzyścią dla organizacji. Należy rozważyć następujące zagadnienia:

- Czy firewall nowej generacji rozszerzy zakres widoczności i ułatwi zrozumienie ruchu sieciowego związanego z aplikacjami?
- Czy będą dostępne opcje zasad reagowania na ruch sieciowy inne niż odrzucenie lub zezwolenie?
- Czy nasza sieć będzie chroniona przed zagrożeniami i atakami w cyberprzestrzeni — znanymi i nieznanymi?
- Czy możemy systematycznie identyfikować nieznany ruch sieciowy i zarządzać nim?
- Czy możemy implementować żądane zasady zabezpieczeń bez niekorzystnego wpływu na wydajność?
- Czy ilość zasobów administracyjnych, przeznaczanych przez zespół firmy na zarządzanie firewallem, zostanie zmniejszona?
- Czy zarządzanie ryzykiem będzie łatwiejsze i bardziej efektywne?
- Czy zasady mogą ułatwić uzyskanie lepszych wyników biznesowych?

W przypadku odpowiedzi „tak" na powyższe pytania decyzja o przejściu od starszych firewalli do firewalli nowej generacji jest uzasadniona. Następnym krokiem jest rozważenie alternatywnych rozwiązań oferowanych przez dostawców firewalli. Podczas oceny dostępnych rozwiązań alternatywnych należy koniecznie zwrócić uwagę na różnice architektoniczne między oferowanymi firewallami nowej generacji oraz związane z nimi implikacje dotyczące rzeczywistych funkcji, procesów i wydajności.

Firewalle nowej generacji

1. **Identyfikowanie aplikacji niezależnie od portu, protokołu, metody obchodzenia zabezpieczeń lub deszyfrowania.**
2. **Identyfikowanie użytkowników niezależnie od urządzenia lub adresu IP.**
3. **Ochrona w czasie rzeczywistym przed znanymi i nieznanymi zagrożeniami związanymi z aplikacjami.**
4. **Zapewnienie szczegółowej widoczności aplikacji, użytkowników i zawartości oraz kontroli opartej na zasadach.**
5. **Zapewnienie przewidywalnego, wielogigabitowego, zgodnego wdrożenia.**

Czynniki architektoniczne związane z klasyfikacją ruchu sieciowego przy użyciu firewalli

Projektując firewalle nowej generacji, dostawcy zabezpieczeń stosują jedną z dwóch koncepcji architektonicznych:

1. Wbudowanie mechanizmu identyfikacji aplikacji w firewall jako podstawowy element klasyfikacyjny.

2. Dodanie elementu dopasowującego wzorce sygnatur aplikacji do firewalla blokującego porty.

Obie metody umożliwiają rozpoznawanie aplikacji, jednak z różną skutecznością, użytecznością i relewantnością. Najważniejszą cechą tych rozwiązań architektonicznych jest określony model zabezpieczeń oparty na zasadach aplikacji — pozytywnych (zezwalanie na określone i blokowanie wszystkich pozostałych) lub negatywnych (blokowanie określonych i zezwalanie na wszystkie pozostałe).

- Pozytywny model zabezpieczeń (firewall lub inne rozwiązanie) umożliwia zapisywanie zasad akceptujących określone aplikacje lub funkcje (np. WebEx, SharePoint, Gmail) i automatyczne odrzucanie innego ruchu. Aby osiągnąć ten poziom kontroli, należy aktywnie klasyfikować całych ruch sieciowy na firewallu (nie później), aby umożliwić akceptowanie odpowiedniego ruchu i odrzucanie pozostałych pakietów. Zapewniając pełną widoczność całego ruchu sieciowego, firmy mogą ograniczać ilość zasobów administracyjnych wymaganych do monitorowania aktywności sieciowej, zarządzania zasadami i analizy wypadków naruszenia systemu zabezpieczeń. Przykładem implikacji związanych z zabezpieczeniami może być bardziej skuteczna ochrona przed znanymi i nieznanymi atakami w cyberprzestrzeni, mimo że akceptowana może być większa liczba aplikacji w sieci, oraz lepsza kontrola nieznanych aplikacji zgodnie z zasadą blokowania całego pozostałego ruchu na firewallu.

- Negatywny model zabezpieczeń (IPS, AV itd.) umożliwia wyszukiwanie i blokowanie określonych zagrożeń lub niepożądanych aplikacji i zezwalanie na pozostały ruch sieciowy. Oznacza to, że ruch sieciowy jest klasyfikowany tylko w zakresie zgodnym z listą blokowanych składników. Ta technika może być skuteczna w przypadku selektywnego wyszukiwania i blokowania zagrożeń lub niepożądanych aplikacji, jednak negatywny model zabezpieczeń jest niedostosowany do pełnienia funkcji głównego elementu kontroli całego ruchu w sieci. Z tego powodu techniki negatywnego modelu zabezpieczeń zostały relegowane do pełnienia jedynie funkcji pomocniczych względem firewalla. Przykładem biznesowych implikacji negatywnego modelu zabezpieczeń może być zwiększenie wymaganej ilości zasobów administracyjnych na skutek dużej liczby zasad i zduplikowanych baz danych logów.

Dalszą część Przewodnika dla klientów podzielono na trzy sekcje. Korzystając z wprowadzenia *10 warunków, które musi spełnić Twój nowy firewall*, zamieszczonego w pierwszej sekcji, można upewnić się, że powyższa architektura i model kontroli umożliwia identyfikowanie i bezpieczne akceptowanie aplikacji na firewallu.
W pozostałych sekcjach szczegółowo omówiono tych 10 warunków, ułatwiających wybór dostawcy przy użyciu zapytania ofertowego i fizyczną ocenę firewalla.

10 warunków, które musi spełnić Twój nowy firewall

Kryteria wyboru firewalla zazwyczaj można podzielić na trzy obszary: funkcje zabezpieczeń, procesy i wydajność. Elementy funkcjonalne zabezpieczeń są związane z ich skutecznością i możliwością zarządzania przez zespół ryzykiem skojarzonym z aplikacjami używanymi w sieci. Z perspektywy procesów podstawowe pytanie to „gdzie zasady aplikacji są rozmieszczone i jak trudne i złożone jest zarządzanie nimi przez zespół?". Różnica funkcjonalna jest prosta: czy firewall może wykonywać zadania przy zachowaniu przepustowości wymaganej przez firmę? W przypadku każdej organizacji obowiązują inne wymagania i priorytety w trzech kryteriach wyboru, jednak obowiązuje następujących 10 warunków, które musi spełnić Twój nowy firewall:

1. **Identyfikowanie i kontrolowanie aplikacji na dowolnym porcie**
2. **Identyfikowanie i kontrolowanie prób obejścia zabezpieczeń**
3. **Deszyfrowanie wychodzących pakietów protokołu SSL i kontrolowanie protokołu SSH**
4. **Zapewnienie kontroli funkcji aplikacji**
5. **Systematyczne zarządzanie nieznanym ruchem sieciowym**
6. **Skanowanie w poszukiwaniu wirusów i złośliwego oprogramowania we wszystkich aplikacjach na wszystkich portach**
7. **Zapewnianie widoczności i kontroli tej samej aplikacji dla wszystkich użytkowników i urządzeń**
8. **Upraszczanie zabezpieczeń sieci, a nie ich komplikacja poprzez dodanie kontroli aplikacji**
9. **Utrzymanie stałej przepustowości i wydajności przy aktywacji pełnej kontroli aplikacji**
10. **Obsługa dokładnie takich samych funkcji firewalla w przypadku systemów sprzętowych i wirtualnych**

1.

Twój nowy firewall musi identyfikować i kontrolować aplikacje równocześnie na wszystkich portach.

Przykład biznesowy: Deweloperzy aplikacji nie muszą już stosować standardowej metodologii projektowej port /protokół/aplikacja. Coraz więcej aplikacji może korzystać z niestandardowych portów lub stosować metodę wymiany portów „port hopping" (np. aplikacje obsługujące wiadomości błyskawiczne, udostępnianie plików w sieciach peer-to-peer lub telefonię internetową przy użyciu protokołu VoIP). Ponadto użytkownicy coraz częściej konfigurują aplikacje do korzystania z niestandardowych portów (np. RDP i SSH). Aby egzekwować zasady firewalla specyficzne dla aplikacji, w których porty są istotne w coraz mniejszym stopniu, Twój nowy firewall musi zakładać, że każda aplikacja może korzystać z dowolnego portu. Koncepcja korzystania z dowolnych portów przez aplikacje jest jedną z fundamentalnych zmian w dziedzinie aplikacji, wymuszającą migrację od firewalli blokujących porty do firewalli nowej generacji. Możliwość wykorzystania dowolnego portu przez aplikacje wyjaśnia również, dlaczego negatywny model kontroli nie jest skuteczny. Jeżeli aplikacja może wybrać dowolny port, produkt oparty na kontroli negatywnej wymagałby wstępnych informacji lub testowania wszystkich sygnatur równocześnie na wszystkich portach.

Wymagania: Należy przyjąć proste założenie, że dowolna aplikacja może korzystać z dowolnego portu, a nowy firewall musi domyślnie nieustannie klasyfikować ruch sieciowy według aplikacji na wszystkich portach. Klasyfikacja ruchu sieciowego na wszystkich portach ma charakter cykliczny. W przeciwnym wypadku kontrola oparta na blokowaniu portów będzie obchodzona przy użyciu tych samych metod, które były przyczyną problemów przez wiele lat.

2.

Twój nowy firewall musi identyfikować i kontrolować oprogramowanie do unikania zabezpieczeń.

Przykład biznesowy: Niewielka liczba aplikacji w sieci może być używana do celowego obchodzenia zasad zabezpieczeń wprowadzonych w celu ochrony cyfrowych zasobów organizacji. Dwie klasy aplikacji można zaliczyć do oprogramowania do obchodzenia zabezpieczeń — zaprojektowane specjalnie w tym celu (np. zewnętrzne serwery proxy i szyfrowane tunele inne niż sieci VPN) i aplikacje, które można w łatwy sposób zaadaptować w celu uzyskania tego samego rezultatu (np. narzędzia do zdalnego zarządzania serwerami/komputerami stacjonarnymi).

- Zewnętrzne serwery proxy i aplikacje obsługujące szyfrowane tunele inne niż sieci VPN są używane do obchodzenia zabezpieczeń przy użyciu różnych metod unikowych. Te aplikacje nie mają żadnego zastosowania biznesowego w sieci, ponieważ są projektowane w celu obchodzenia zabezpieczeń, i powodują zagrożenie firmy i systemu zabezpieczeń.

- Narzędzia do zdalnego zarządzania serwerami/komputerami stacjonarnymi (np. RDP i Teamviewer) są zazwyczaj używane przez personel działu pomocy technicznej oraz informatyków do zwiększania wydajności. Są one również często używane przez pracowników do omijania firewalla albo ustanawiania połączeń z komputerami domowymi lub innymi komputerami poza siecią firmy. Osoby dokonujące ataków w cyberprzestrzeni wiedzą, że te aplikacje są powszechnie używane i opublikowano już zarówno w raportach DBIR (Verizon Data Breach Report), jak i raportach Mandiant opisy przypadków wykorzystania tych narzędzi dostępu zdalnego na co najmniej jednym etapie procesu ataku sieciowego.

Nie wszystkie aplikacje tego typu są jednak związane z takimi samymi zagrożeniami — aplikacje dostępu zdalnego mogą być używane do legalnych celów, podobnie jak wiele aplikacji tuneli szyfrowanych. Te same narzędzia są jednak coraz częściej wykorzystywane przez osoby dokonujące wielokrotnie ataków sieciowych. Bez możliwości kontrolowania tych narzędzi do obchodzenia zabezpieczeń organizacje nie mogą egzekwować swoich zasad zabezpieczeń i są narażone na zagrożenia, które, jak im się wydawało, zostały wyeliminowane.

Wymagania: Istnieją różnego typu aplikacje do obchodzenia zabezpieczeń, stosujące nieznacznie różniące się metody. Dostępne są zarówno publiczne, jak i prywatne zewnętrzne serwery proxy (w witrynie proxy.org zamieszczono obszerną bazę danych publicznych serwerów proxy), które mogą korzystać z protokołów HTTP i HTTPS. Prywatne serwery proxy są często konfigurowane do korzystania z nieklasyfikowanych adresów IP (np. komputery domowe) przy użyciu aplikacji takich jak PHProxy lub CGIProxy. Aplikacje dostępu zdalnego (np. RDP, Teamviewer lub GoToMyPC) mogą być używanego do legalnych celów, jednak ze względu na skojarzone ryzyko należy nimi zarządzać z ostrożnością. Większość innych aplikacji umożliwiających obejście zabezpieczeń (np. Ultrasurf, Tor, Hamachi) nie ma zastosowań biznesowych w sieci firmy. Niezależnie od zasad zabezpieczeń obowiązujących w firmie nowy firewall musi identyfikować i kontrolować wszystkie aplikacje tego typu, niezależnie od portu, protokołu, szyfrowania lub metody unikowej. Dodatkowe zalecenie: aplikacje umożliwiające obchodzenie zabezpieczeń są regularnie aktualizowane w celu utrudnienia wykrywania ich i kontrolowania. Należy więc koniecznie nie tylko pamiętać, że nowy firewall musi identyfikować aplikacje obchodzące zabezpieczenia, ale również wiedzieć, jak często algorytmy tej aplikacji są aktualizowane i korygowane.

3.

Twój nowy firewall musi deszyfrować i sprawdzać pakiety protokołu SSL i kontrolować protokół SSH.

Przykład biznesowy: Obecnie 26% aplikacji używa protokołu SSL przy użyciu jakiejś metody lub formy we współczesnych sieciach firmowych[2]. Uwzględniając rozpowszechnienie protokołu HTTPS w wielu rentownych aplikacjach wysokiego ryzyka, z których korzystają użytkownicy końcowi (np. Gmail i Facebook), oraz możliwość wymuszania protokołu SSL przez użytkowników w wielu witrynach, zespół firmy ds. zabezpieczeń musi pomijać coraz większy obszar bez możliwości deszyfrowania, kontrolowania i skanowania ruchu sieciowego zaszyfrowanego przy użyciu protokołu SSL. Z pewnością firewall nowej generacji musi być dostatecznie elastyczna, aby umożliwiać pomijanie zaszyfrowanego ruchu sieciowego SSL określonego typu (np. ruch sieci Web z usług finansowych lub organizacji służby zdrowia), a jednocześnie deszyfrowanie zgodnie z zasadami ruchu innego typu (np. SSL na portach niestandardowych, HTTPS z nieklasyfikowanych witryn sieci Web w Europie Wschodniej). Protokół SSH jest używany prawie uniwersalnie i może być w łatwy sposób skonfigurowany przez użytkowników końcowych do celów niezwiązanych z pracą w taki sam sposób, jak narzędzie pulpitu zdalnego. Szyfrowanie protokołu SSH umożliwia wykorzystanie go do ukrywania działań niezwiązanych z pracą.

Wymagania: Możliwość deszyfrowania protokołu SSL jest fundamentalnym czynnikiem — nie tylko dlatego, że pakiety tego typu stanowią coraz większy odsetek ruchu sieciowego w przedsiębiorstwach, ale również z powodu kilku innych ważnych funkcji, które byłyby niekompletne lub nieefektywne bez możliwości deszyfrowania protokołu SSL. Najważniejsze elementy to rozpoznawanie i deszyfrowanie SSL na dowolnym porcie dla ruchu przychodzącego i wychodzącego, kontrola zasad dla deszyfrowania oraz niezbędne składniki sprzętu i oprogramowania umożliwiające deszyfrowanie równocześnie kilkudziesięciu tysięcy połączeń SSL z przewidywalną wydajnością. Dodatkowe wymagania, które należy rozważyć, to możliwość identyfikowania i kontrolowania użycia protokołu SSH. W szczególności kontrola protokołu SSH powinna uwzględniać możliwość ustalenia, czy jest on używany do przekierowania portów (lokalny, zdalny, X11) lub zastosowania macierzystego (SCP, SFTP i dostęp do powłoki). Po ustaleniu, jak protokół SSH jest używany, można przygotować odpowiednie zasady zabezpieczeń.

4.

Twój nowy firewall musi zapewniać kontrolę funkcji aplikacji.

Przykład biznesowy: Deweloperzy platformy aplikacji takich jak Google, Facebook, Salesforce.com lub Microsoft oferują wiele funkcji, które ułatwiają pozyskanie lojalnych użytkowników, jednak mogą być związane z różnymi profilami ryzyka. Na przykład można zezwolić na korzystanie z użytecznego narzędzia biznesowego Webex, jednak użycie funkcji udostępniania pulpitu Webex do przejęcia kontroli nad komputerem stacjonarnym pracownika ze źródła zewnętrznego może spowodować naruszenie rozporządzeń wewnętrznych lub zasad zgodności z przepisami. Innym przykładem może być Google Mail (Gmail) i Google Talk (Gtalk). Po zalogowaniu użytkownika w usłudze Gmail, która może być dozwolona w zasadach, możne on w łatwy sposób przełączyć kontekst do usługi Gtalk, która powinna być zablokowana. Twój nowy firewall musi rozpoznawać i klasyfikować indywidualne funkcje i umożliwiać wdrożenie odpowiednich zasad reagowania.

Wymagania: Twój nowy firewall musi nieustannie klasyfikować poszczególne aplikacje i monitorować zmiany, które mogą oznaczać, że używana jest inna funkcja. Koncepcja „jednorazowej" klasyfikacji nie jest opcją, którą można zaakceptować, ponieważ ignoruje fakt, że te powszechnie używane aplikacje korzystają ze wspólnych sesji i obsługują wiele funkcji. Jeżeli inna funkcja zostanie wprowadzona w sesji, firewall musi odnotować tę zmianę w tabelach stanu i sprawdzić zasady. Podstawowym wymaganiem dotyczącym nowego firewalla jest nieustanne śledzenie stanu w celu zrozumienia funkcji obsługiwanych przez poszczególne aplikacje i skojarzonego ryzyka.

Bezpieczne korzystanie z aplikacji
Aby bezpiecznie wykorzystać aplikacje i technologie do prowadzenia działalności biznesowej, zespoły ds. zabezpieczeń sieciowych muszą nie tylko wdrożyć odpowiednie zasady użytkowania, ale również metody egzekwowania tych zasad.

[2] Raport dotyczący użycia aplikacji i zagrożeń Palo Alto Networks, styczeń 2013

5.

Twój nowy firewall musi systematycznie zarządzać nieznanym ruchem sieciowym.

Przykład biznesowy: Nieznany ruch sieciowy występuje w niewielkich ilościach w każdej sieci, jednak stanowi poważne zagrożenie dla użytkowników i organizacji. Należy rozważyć kilka istotnych zagadnień związanych z nieznanym ruchem sieciowym — czy jest dzielony na kategorie, czy można minimalizować go przy użyciu zasad, czy firewall może w łatwy sposób charakteryzować niestandardowe aplikacje i umożliwia zaklasyfikowanie ich jako „znane" w kontekście lokalnych zasad zabezpieczeń i czy firewall ułatwia określenie zagrożenia związanego z nieznanym ruchem?

Nieznany ruch jest również silnie związany z zagrożeniami w sieci. Osoby dokonujące ataków sieciowych są często zmuszone do modyfikowania protokołu w celu wykorzystania luk w zabezpieczeniach aplikacji. Na przykład, aby zaatakować serwer sieci Web, atakujący musi zmodyfikować nagłówek protokołu HTTP do tego stopnia, że wynikowy ruch sieciowy nie jest już identyfikowany jako ruch sieci Web. Anomalie tego typu są wczesnym sygnałem zbliżającego się ataku. Podobnie złośliwe oprogramowanie często używa dostosowanych protokołów w swoim modelu poleceń i sterowania, umożliwiając zespołom ds. zabezpieczeń stłumienie w zarodku każdej infekcji związanej z nieznanym złośliwym oprogramowaniem.

Wymagania: Domyślny nowy firewall musi klasyfikować cały ruch sieciowy na wszystkich portach — w tym obszarze wcześniejsza dyskusja dotycząca architektury i modelu kontroli zabezpieczeń jest bardzo ważna. Pozytywne (domyślne odrzucanie) modele klasyfikują wszystko, a negatywne (domyślne zezwalanie) modele klasyfikują tylko składniki zgodne z zaleceniami. Klasyfikowanie całego ruchu sieciowego jest tylko drobnym aspektem problemu związanego z nieznanym ruchem. Nowy firewall musi umożliwiać monitorowanie całego nieznanego ruchu sieciowego na wszystkich portach w pojedynczej lokalizacji [zarządzania] i szybko analizować ruch w celu ustalenia, czy jest to (1) aplikacja wewnętrzna lub niestandardowa, (2) aplikacja komercyjna bez sygnatury czy (3) zagrożenie. Dodatkowo nowy firewall musi udostępniać wszystkie niezbędne narzędzia umożliwiające nie tylko monitorowanie nieznanego ruchu sieciowego, ale również systematyczne zarządzanie nim przy użyciu zasad, tworzenie niestandardowej sygnatury, przesyłanie PCAP aplikacji komercyjnej w celu dalszej analizy lub przeprowadzenia dochodzenia w przypadku zagrożenia.

6.

Twój nowy firewall w poszukiwaniu zagrożeń musi skanować wszystkie aplikacje na wszystkich portach.

Przykład biznesowy: Przedsiębiorstwa nieustannie adaptują do działalności biznesowej wiele aplikacji, które mogą być obsługiwane wewnątrz lub na zewnątrz siedziby lokalizacji przedsiębiorstwa. W przypadku hostowanych usług SharePoint, Box.net, Google Docs lub Microsoft Office365, a nawet aplikacji sieci ekstranet obsługiwanych przez partnera wiele organizacji wymaga użycia aplikacji, która może korzystać z niestandardowych portów, protokołu SSL lub funkcji udostępniania plików. Mówiąc inaczej, te aplikacje umożliwiają prowadzenie działalności biznesowej, jednak mogą być również związane z zagrożeniem w cyberprzestrzeni. Ponadto niektóre z tych aplikacji (np. SharePoint) wykorzystują technologie pomocnicze, które są często obiektem ataków (np. IIS i SQL Server). Blokowanie aplikacji nie jest odpowiednim rozwiązaniem, podobnie jak bezwarunkowe zezwalanie na korzystanie z aplikacji z (potencjalnymi) skojarzonymi zagrożeniami w środowisku biznesowym i cyberprzestrzeni.

Ta tendencja do korzystania z niestandardowych portów jest bardzo widoczna w środowisku złośliwego oprogramowania. Od momentu, gdy złośliwe oprogramowanie znajdzie się w sieci, a większość takich przypadków wymaga uczestnictwa klienta (złośliwe oprogramowanie) komunikującego się z serwerem C&C, atakujący może swobodnie wybierać dowolną kombinację portu i protokołu. W rzeczywistości na podstawie analizy trzech ubiegłych miesięcy ustalono, że 97% nieznanego złośliwego oprogramowania przekazanego za pośrednictwem FTP korzystało z całkowicie niestandardowych portów.

Wymagania: Aby umożliwić bezpieczne korzystanie z aplikacji, należy ją zaakceptować i skanować w poszukiwaniu zagrożeń. Te aplikacje mogą komunikować się za pośrednictwem kombinacji protokołów (np. program SharePoint korzysta z protokołów CIFS, HTTP i HTTPS i wymaga zasad firewalla bardziej złożonych niż „blokuj aplikację"). Pierwszym krokiem jest identyfikacja aplikacji (niezależnie od portu i szyfrowania), ustalenie funkcji, które należy zaakceptować lub zablokować, a następnie skanowanie zaakceptowanych składników w poszukiwaniu zagrożeń — luk w zabezpieczeniach, wirusów/oprogramowania złośliwego lub szpiegującego, a nawet ważnych, kontrolowanych lub poufnych informacji.

7.

Twój nowy firewall musi zapewniać spójną kontrolę wszystkich użytkowników niezależnie od lokalizacji lub typu urządzenia.

Przykład biznesowy: Twoi użytkownicy coraz częściej przebywają poza siedzibą przedsiębiorstwa i często uzyskują dostęp do sieci firmy przy użyciu smartfonów lub tabletów. Kiedyś była to domena osób podróżujących służbowo, a obecnie znaczna część personelu może pracować zdalnie. Użytkownicy pracujący w kawiarni, domu lub siedzibie klienta oczekują na możliwość połączenia się z ich aplikacjami za pośrednictwem sieci WiFi, bezprzewodowego modemu szerokopasmowego lub innych metod. Niezależnie od lokalizacji użytkownika, a nawet rozmieszczenia jego aplikacji, powinien obowiązywać ten sam standard kontroli przy użyciu firewalla. Jeżeli nowy firewall zapewnia widoczność aplikacji i kontrolę ruchu sieciowego w siedzibie przedsiębiorstwa, ale nie poza nią, pomija ruch związany z największymi zagrożeniami.

Wymagania: Jest to prosta koncepcja — nowy firewall musi zapewniać spójną widoczność i kontrolę ruchu sieciowego niezależnie od lokalizacji użytkownika. Nie oznacza to, że organizacja musi stosować dokładnie te same zasady w obu wypadkach. Na przykład niektóre organizacje zezwalają pracownikom na korzystanie z usługi Skype podczas podróży służbowych, ale nie w siedzibie głównej, a inne mogą wprowadzić zasady zezwalające użytkownikom znajdującym się poza biurem na pobieranie załączników Salesforce.com pod warunkiem, że włączono funkcji szyfrowania ich dysków twardych. Twój nowy firewall powinien być przystosowany do takiej konfiguracji bez znacznego opóźnienia obsługi użytkowników końcowych, zbędnego obciążenia administratora lub znacznego kosztu dla organizacji.

8.

Twój nowy firewall musi upraszczać zabezpieczenia sieci dzięki dodatkowej kontroli aplikacji.

Przykład biznesowy: Wiele przedsiębiorstw ma problemy z wdrożeniem dodatkowych źródeł informacji, zasad i procedur zarządzania w przeciążonych procesach zabezpieczeń i harmonogramach personelu. Mówiąc inaczej, jeżeli personel nie może zarządzać zasobami, którymi obecnie dysponuje, dodanie urządzeń, interfejsów zarządzania ze skojarzonymi zasadami oraz źródeł informacji nie ułatwi ograniczenia obciążenia personelu zadaniami administracyjnymi i nie przyśpieszy reagowania na zgłoszenia dotyczące problemów technicznych. Im bardziej rozproszone zasady (np. firewall blokujący porty zezwala na ruch sieciowy przez port 80, system IPS wyszukuje/blokuje zagrożenia i aplikacje, a bezpieczna brama sieci Web filtruje adresy URL), tym trudniej jest zarządzać tymi zasadami. Jakich zasad zespół ds. zabezpieczeń używa do udostępniania usługi WebEx? Jak są identyfikowane i rozwiązywane konflikty zasad na różnych urządzeniach? Zakładając, że w instalacjach z typowym firewallem blokującym porty obowiązują tysiące reguł, dodanie tysięcy sygnatur aplikacji na kilkudziesięciu tysiącach portów spowoduje znaczne podwyższenie stopnia złożoności.

Wymagania: Firma jest zależna od aplikacji, użytkowników i zawartości, a Twój nowy firewall musi zezwalać na tworzenie zasad bezpośrednio wspierających Twoje inicjatywy biznesowe. Wspólny kontekst między aplikacją, użytkownikiem a zawartością we wszystkich aspektach (widoczność, kontrolowanie przy użyciu zasad, rejestrowanie w logach i raporty) znacznie ułatwi uproszczenie infrastruktury zabezpieczeń. Połączenie zasad firewalla opartych na portach i adresach IP, oddzielnych zasad kontrolowania aplikacji, systemu IPS i eliminacji złośliwego oprogramowania komplikuje proces zarządzania zasadami i może ograniczać wydajność w firmie.

9.

Twój nowy firewall musi zapewniać stałą przepustowość i wydajność po pełnym uaktywnieniu kontroli aplikacji.

Przykład biznesowy: Wiele organizacji usiłuje osiągnąć kompromis pomiędzy wydajnością a bezpieczeństwem. Zbyt często włączenie nowych funkcji zabezpieczeń na firewallu powoduje znaczne zmniejszenie przepustowości i wydajności. Jeżeli firewall nowej generacji jest prawidłowo zaprojektowana, ten kompromis nie jest konieczny.

Wymagania: Znaczenie architektury jest oczywiste również w tym wypadku, ale w inny sposób. Połączenie ze sobą firewalla blokującego porty z funkcjami zabezpieczeń wykorzystującymi inną technologię zazwyczaj oznacza występowanie zbędnych warstw sieci, modułów skanujących i zasad, a w rezultacie niedostateczną wydajność. Z perspektywy oprogramowania firewall musi być zaprojektowany ze wszystkimi tymi funkcjami w podstawowej konfiguracji. Ponadto, uwzględniając wymagania dotyczące mocy obliczeniowej (np. identyfikacja aplikacji, zapobieganie zagrożeniom na wszystkich portach itd.) przy dużym natężeniu ruchu sieciowego i niskiej tolerancji na opóźnienie związane z ochroną krytycznej infrastruktury, nowy firewall musi mieć również odpowiedni sprzęt (dedykowany, przystosowany do pracy w sieci z zabezpieczeniami i skanowaniem zawartości).

10.

Twój nowy firewall musi obsługiwać dokładnie takie same funkcje kontroli w przypadku systemów sprzętowych i wirtualnych.

Przykład biznesowy: Szybki rozwój wirtualizacji i środowiska chmury komputerowej jest związany z nowymi zagrożeniami dla systemów zabezpieczeń. Efektywne rozwiązanie tych problemów przy użyciu starszych firewalli jest utrudnione lub niemożliwe za względu na niespójność funkcjonalną, rozproszone zarządzanie i brak punktów integracji ze środowiskiem wirtualizacji. Aby chronić ruch sieciowy przepływający do i od centrum danych i w środowiskach wirtualnych, nowy firewall musi obsługiwać dokładnie takie same funkcje w przypadku systemów sprzętowych i wirtualnych.

Wymagania: Dynamiczne uruchamianie i deaktywacja aplikacji w wirtualnym centrum danych utrudnia identyfikowanie i kontrolowanie aplikacji przy użyciu metody blokowania portów i adresów IP. Oprócz funkcji opisanych w sekcji *10 warunków, które musi spełnić Twój nowy firewall* w systemach sprzętowych i wirtualnych wymagana jest ścisła integracja ze środowiskiem wirtualizacji umożliwiająca usprawnienie tworzenia zasad dotyczących aplikacji po dodaniu lub usunięciu komputerów wirtualnych i aplikacji. Jest to jedyna metoda zapewnienia obsługi ewoluujących architektur centrów danych z elastycznością operacyjną, a jednocześnie uwzględniających zagrożenia i wymagania dotyczące zgodności.

Firewalle powinny umożliwiać bezpieczne wykorzystanie aplikacji do działalności biznesowej

Użytkownicy nieustannie adaptują nowe aplikacje i technologie, często wykorzystując je do pracy, jednak nie uwzględniają skojarzonych zagrożeń dla firmy i systemu zabezpieczenia. W niektórych wypadkach zablokowanie tych aplikacji przez zespół ds. zabezpieczeń może nawet utrudnić prowadzenie działalności biznesowej.

Aplikacje są używane przez personel do pracy i umożliwiają utrzymanie produktywności zgodnie z priorytetami osobistymi i zawodowymi. Zgodnie z obecnymi zaleceniami system zabezpieczeń powinien więc umożliwiać bezpieczne korzystania z aplikacji. Aby bezpiecznie wykorzystać aplikacje i technologie w sieci do prowadzenia działalności biznesowej, zespoły ds. zabezpieczeń sieciowych muszą nie tylko wdrożyć odpowiednie zasady użytkowania, ale również metody egzekwowania tych zasad.

W sekcji *10 warunków, które musi spełnić Twój nowy firewall* opisano najważniejsze funkcje umożliwiające organizacjom bezpieczne korzystanie z aplikacji i prowadzenie działalności biznesowej. Następnym krokiem jest opracowanie procedur na podstawie tych wymagań, wybór dostawcy przy użyciu procesu RFP i formalna ocena oferowanych rozwiązań, a następnie zakup i wdrożenie firewalla nowej generacji.

Prowadzenie działalności biznesowej
We współczesnym nieustannie połączonym środowisku online kontrolowanie aplikacji nie ogranicza się do akceptowania lub odrzucania. Celem jest umożliwienie bezpiecznego wykorzystania aplikacji do prowadzenia działalności biznesowej.

Wybór firewalla nowej generacji przy użyciu procesu RFP

Zazwyczaj podczas wyboru firewalli, systemów IPS lub innych ważnych składników infrastruktury zabezpieczeń organizacje rozsyłają zapytania ofertowe (RFP) gwarantujące, że zostaną spełnione ich specyficzne wymagania. Zgodnie z Gartner Magic Quadrant for Enterprise Firewalls „zmienne zagrożenia, warunki biznesowe i procesy IT zmuszają menedżerów zabezpieczeń sieciowych do poszukiwania firewalli nowej generacji w najbliższym cyklu wymiany firewalla/systemu IPS". Przy najbliższej okazji do wdrożenia nowych rozwiązań organizacje powinny uwzględnić w swojej dokumentacji RFP funkcje związane z widocznością i kontrolowaniem aplikacji, dostępne w rozwiązaniach nowej generacji. W poprzedniej sekcji omówiono 10 najważniejszych wymagań, które musi spełnić Twój nowy firewall. W tej sekcji omówimy przygotowanie na podstawie tych wymagań narzędzi umożliwiających identyfikację i wybór firewalla nowej generacji.

Architektura firewalla i model kontroli

Aby ustalić, czy firewall oferowany przez dostawcę umożliwia efektywne monitorowanie i kontrolowanie aplikacji, należy rozważyć kilka czynników. Architektura firewalla, a w szczególności aparat klasyfikacji ruchu sieciowego określa efektywność identyfikacji i kontroli aplikacji, uzupełniającej filtrowanie portów i protokołów. Jak już wspomniano, nowy firewall każdego typu musi przede wszystkim precyzyjnie klasyfikować ruch sieciowy, a następnie na tej podstawie podejmować wszystkie decyzje związane z zasadami zabezpieczeń.

W tym modelu firewall stosuje tradycyjny pozytywny model kontroli (blokowanie wszystkich z wyjątkiem wyraźnie dozwolonych przez użytkownika). Pozytywny model umożliwia kontrolowanie i udostępnianie aplikacji zgodnie z podstawowym wymaganiem we współczesnym, nieustannie aktywnym i połączonym biznesowym środowisku online. Wyszukiwanie aplikacji przy użyciu systemów typu IPS oznacza, że używany jest negatywny model kontroli (zezwalanie na wszystko z wyjątkiem składników wyraźnie odrzuconych przez system IPS). Negatywny model umożliwia tylko blokowanie aplikacji. Różnice są analogiczne do włączenia światła w pokoju do kontrolowania wszystkich składników (model pozytywny) i korzystania z latarki w pokoju w celu monitorowania i kontrolowania tylko wybranych składników (model negatywny). Użycie tego dodatku do identyfikowania i blokowania „nieodpowiednich" pakietów jest po prostu poprawką, a nie pełnym rozwiązaniem, ponieważ umożliwia monitorowanie tylko części ruchu sieciowego w celu uniknięcia ograniczenia wydajności i nie uwzględnia wszystkich ataków i aplikacji w cyberprzestrzeni.

Widoczność i kontrolowanie aplikacji

Zapytanie ofertowe (RFP) musi zawierać szczegółowe informacje dotyczące architektury firewalla umożliwiającej identyfikowanie i kontrolowanie pełnego spektrum aplikacji biznesowych, osobistych i innych oraz protokołów niezależnie od portu, szyfrowania SSL lub stosowanej metody obchodzenia zabezpieczeń. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Aby uniknąć wykrycia, wiele aplikacji korzysta z niestandardowych portów, metody wymiany portów (port hopping) lub konfiguracji umożliwiającej użycie innego portu.
  - Czy mechanizmy identyfikowania aplikacji zostały uwzględnione w module klasyfikacji ruchu sieciowego firewalla (tzn. są domyślnie włączone)?
  - Czy mechanizmy identyfikowania firewalla są zależne od standardowego portu aplikacji?
  - Czy można stosować sygnatury w odniesieniu do wszystkich portów i czy ten proces jest konfigurowany automatycznie czy ręcznie?
- Czy ruch sieciowy odbierany przez urządzenie jest najpierw klasyfikowany na podstawie portu („to jest port 80, a więc można uznać, że ruch jest związany z protokołem HTTP") czy aplikacji („to jest usługa Gmail")?
- Proszę opisać szczegółowo, jak firewall może precyzyjnie identyfikować aplikacje.
  - Jakie mechanizmy oprócz sygnatur są używane do klasyfikowania ruchu sieciowego?
  - Proszę opisać typy aplikacji i zastosowania dekodera protokołów.
  - Jak wdrożono deszyfrowanie i kontrolowanie protokołów SSL i SSH?
  - Czy mechanizmy klasyfikacji ruchu sieciowego są stosowane w równym stopniu w odniesieniu do wszystkich portów?
- Jakie mechanizmy są używane do wykrywania aplikacji obchodzących zabezpieczenia, takich jak UltraSurf lub szyfrowane połączenia P2P?
- Czy aplikacje są identyfikowane na firewallu czy w dodatkowym procesie po klasyfikacji na podstawie portów?
  - Jakie są trzy najważniejsze zalety zastosowanej architektury?
- Czy stan aplikacji jest śledzony, a jeżeli tak, to jak te informacje są wykorzystywane do zapewnienia spójnej kontroli aplikacji i skojarzonych funkcji pomocniczych?
  - Proszę podać trzy przykłady wykorzystania informacji dotyczących stanu aplikacji w zasadach zabezpieczeń.
- Czy tożsamość aplikacji jest podstawą zasad zabezpieczeń firewalla czy kontrola aplikacji jest tylko podrzędnym elementem zasad?
- Jak często jest aktualizowana baza danych aplikacji i czy jest to aktualizacja dynamiczna czy uaktualniana podczas ponownego uruchamiania systemu?
- Jak ruch sieciowy jest klasyfikowany przez system wirtualny w środowiskach wirtualnych (wschód/zachód, północ/południe).
  - Proszę opisać punkty integracji w środowisku wirtualnym.
  - Proszę opisać proces tworzenia zasad zabezpieczeń dla nowych maszyn wirtualnych.
  - Proszę opisać dostępne funkcje śledzenia zmiany lokalizacji, dodawania składników i zmian maszyn wirtualnych.
  - Proszę opisać dostępne funkcje integracji z systemami automatyzacji i instrumentacji środowiska wirtualnego.

Kontrolowanie aplikacji obchodzących zabezpieczenia oraz protokołów SSL i SSH

Wiele aplikacji można wykorzystać do obejścia zabezpieczeń. Niektóre aplikacje, takie jak zewnętrzne serwery proxy i szyfrowane tunele niezwiązane z sieciami VPN, zaprojektowano specjalnie w celu obchodzenia zabezpieczeń. Inne aplikacje, takie jak narzędzia do zdalnego zarządzania serwerami/komputerami stacjonarnymi, ewoluowały do postaci, w której personel inny niż informatycy lub pracownicy działu pomocy technicznej może używać ich do obchodzenia mechanizmów kontrolnych. Protokół SSL jest obecnie standardowym elementem konfiguracji zabezpieczeń wielu aplikacji dla użytkowników końcowych, jednak protokół SSL może maskować zagrożenia związane z przychodzącym lub wychodzącym ruchem związanym z przesyłaniem danych. Obecnie około 26% aplikacji używanych w sieci może korzystać z protokołu SSL[3] w pewnym zakresie. Należy więc koniecznie zidentyfikować odpowiednich dostawców firewalli nowej generacji, którzy uwzględnili tę kategorię aplikacji. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Proszę opisać proces identyfikowania aplikacji z szyfrowaniem SSL na wszystkich portach, łącznie z portami niestandardowymi.
- Jakie dostępne zasady zabezpieczeń umożliwiają selektywne deszyfrowanie, sprawdzanie i kontrolowanie aplikacji korzystających z protokołu SSL?
- Czy obsługiwana jest dwukierunkowa identyfikacja, odszyfrowywanie oraz inspekcja protokołu SSL?
- Czy deszyfrowanie SSL jest funkcją standardową czy związaną z dodatkową opłatą? Czy wymagane jest dedykowane urządzenie?
- Narzędzie SSH jest powszechnie używane do uzyskiwania dostępu do urządzeń zdalnych przez informatyków, personel działu pomocy technicznej i pracowników, którzy interesują się nowymi technologiami.
  - Proszę szczegółowo opisać kontrolę SSH, jeżeli jest obsługiwana?
- Jakie mechanizmy są używane do identyfikowania aplikacji obchodzących zabezpieczenia, takich jak UltraSurf lub Tor?
- Proszę opisać automatyczną identyfikację aplikacji obchodzącej zabezpieczenia przy użyciu niestandardowego portu.

[3] Raport dotyczący użycia aplikacji i zagrożeń Palo Alto Networks, styczeń 2013

Filtrowanie aplikacji przy użyciu zasad

We współczesnym nieustannie połączonym środowisku online kontrolowanie aplikacji nie ogranicza się do akceptowania lub odrzucania. Celem jest umożliwienie bezpiecznego wykorzystania aplikacji do prowadzenia działalności biznesowej. Wiele „platform" (Google, Facebook, Microsoft) udostępnia różne aplikacje użytkownikom po wstępnym zalogowaniu. Należy koniecznie ustalić, jak dostawca firewalla monitoruje stan aplikacji, wykrywa zmiany w aplikacji i klasyfikuje zmianę stanu. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Czy klasyfikacja ruchu sieciowego z wykorzystaniem inspekcji stanu jest wykonywana oddzielnie przed identyfikacją aplikacji, a jeżeli tak, proszę opisać jak zmiany stanu aplikacji po zidentyfikowaniu aplikacji są monitorowane, śledzone i wykorzystywane w zasadach.
- Proszę opisać, jak hierarchia bazy danych aplikacji (prosta, wielopoziomowa, inna) ujawnia funkcje w aplikacji macierzystej umożliwiające tworzenie bardziej precyzyjnych zasad akceptowania aplikacji.
- Proszę opisać poziomy kontroli, które można zastosować w odniesieniu do indywidualnych aplikacji oraz ich funkcji:
  - zezwalanie,
  - zezwalanie zależnie od aplikacji, funkcji aplikacji, kategorii, podkategorii, technologii lub ryzyka,
  - zezwalanie na podstawie harmonogramu, użytkownika, grupy, portu,
  - zezwalanie i skanowanie w poszukiwaniu wirusów, luk w zabezpieczeniach aplikacji, oprogramowania szpiegującego, złośliwych pakietów do pobrania,
  - zezwalanie i kształtowanie/stosowanie mechanizmów kontroli jakości usługi,
  - odrzucanie.

- Czy można wdrażać zabezpieczenia oparte na portach dla wszystkich aplikacji w bazie danych, a administrator może egzekwować relacje między aplikacją a portami dla poszczególnych zasad? Przykład:
  - Wymuszone kierowanie deweloperów baz danych Oracle do określonego portu lub zakresu portów?
  - Należy upewnić się, że tylko informatycy mogą korzystać z protokołów SSH i RDP.
  - Wykrywanie i blokowanie złośliwego oprogramowania w aplikacji, nawet w przypadku portu niestandardowego.
- Proszę wymienić wszystkie repozytoria tożsamości w przedsiębiorstwie dostępne dla zabezpieczeń opartych na użytkownikach.
- Czy interfejs API jest dostępny dla niestandardowej integracji infrastruktury tożsamości?
- Proszę opisać jak zabezpieczenia oparte na zasadach są wdrażane dla użytkowników i grup w środowiskach usług terminalowych.
- Proszę opisać ewentualne różnice opcji akceptowania aplikacji dla urządzeń sprzętowych i wirtualnych.

Systematyczne zarządzanie nieznanymi aplikacjami

W każdej sieci występuje nieznany ruch, który zazwyczaj jest związany z aplikacją wewnętrzną lub niestandardową, jednak może to być również niezidentyfikowana aplikacja komercyjna, a w niekorzystnym scenariuszu nawet złośliwe oprogramowanie. Najważniejsze informacje, które można uzyskać przy użyciu zapytania ofertowego (RFP) i procesu ewaluacji, to szczegółowy opis oferowanej przez dostawcę metody systematycznego zarządzania nieznanym ruchem sieciowym, związanym z większym ryzykiem dla firmy i systemu zabezpieczeń. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Proszę szczegółowo opisać, jak można identyfikować nieznany ruch sieciowy w celu analizy.
- Czy mechanizmy używane do analizy uwzględniono w standardowym zestawie funkcji czy też są pomocniczymi, dodatkowymi produktami?
- Jakie warunkowe działania można podejmować w odniesieniu do nieznanego ruchu (zezwalanie, odrzucanie, inspekcja, kształtowanie itd.)?
- Proszę opisać zalecane najlepsze procedury zarządzania nieznanym ruchem sieciowym związanym z aplikacjami.
  - Czy uwzględniono kontrolę przy użyciu zasad podobnie jak w przypadku oficjalnie obsługiwanej aplikacji (np. zezwalanie, odrzucanie, inspekcja, kształtowanie, kontrolowanie według użytkownika, strefy itd.)?
  - Czy można „zmienić nazwę" wewnętrznego ruchu sieciowego?
  - Czy można utworzyć niestandardową sygnaturę aplikacji?
- Jaki proces zastosowano do przesyłania żądań dotyczących nowych lub zaktualizowanych sygnatur aplikacji?
- Ile trwa oczekiwanie na uzyskanie sygnatur nowych aplikacji po przesłaniu wniosku?
- Jakie dostępne mechanizmy umożliwiają ustalenie, czy nieznany ruch sieciowy jest złośliwym oprogramowaniem?

Zapobieganie zagrożeniom

Coraz częściej z aplikacjami są związane zagrożenia takie jak luki w zabezpieczeniach, brak odporności na infekcje komputerowe oraz brak bieżącego sterowania i kontroli zainfekowanych urządzeń. Z tego powodu analitycy zgodnie zalecają przedsiębiorstwom konsolidację tradycyjnych systemów IPS i technologii zapobiegania zagrożeniom jako składnika firewalla nowej generacji. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Proszę opisać wszystkie stosowane mechanizmy zapobiegania zagrożeniom (system IPS, program antywirusowy, program do ochrony przed oprogramowaniem szpiegującym, filtrowanie adresów URL, filtrowanie danych itd.).
- Jak są licencjonowane te mechanizmy zapobiegania zagrożeniom?
- Proszę opisać mechanizmy zapobiegania zagrożeniom opracowane w firmie lub uzyskane za pośrednictwem strony trzeciej lub usługi.
- Jakie zastosowano metody zapobiegania zagrożeniom związanym z aplikacjami korzystającymi z niestandardowych portów?
- Czy informacje związane z identyfikacją aplikacji są zintegrowane czy użytkowane wspólnie z technologiami zapobiegania zagrożeniom? Jeżeli tak, proszę opisać poziom integracji.
- Proszę wymienić dziedziny zapobiegania zagrożeniom (IPS, AV itd.) oparte na portach, a nie aplikacjach.
- Czy aparat zapobiegania zagrożeniom skanuje zawartość skompresowanych plików takich jak ZIP lub GZIP?
- Czy aparat zapobiegania zagrożeniom może skanować w zawartości szyfrowanej przy użyciu protokołu SSL?
- Proszę wyjaśnić, jak firewall może wykrywać niestandardowe lub polimorficzne złośliwe oprogramowanie i zapewnić ochronę przez nim.
  - Jakie mechanizmy są używane do blokowania złośliwego oprogramowania?
- Proszę opisać proces badań i prac rozwojowych związanych z zapobieganiem zagrożeniom.

Ochrona użytkowników zdalnych

Użytkownicy nowoczesnych sieci oczekują możliwości ustanawiania połączenia i pracy z wielu lokalizacji poza tradycyjną granicą sieci. Należy zapewnić ochronę tych użytkowników nawet wówczas, gdy znajdują się poza granicami sieci i korzystają z komputera, smartfonu lub tabletu. Celem tej sekcji jest ustalenie, jakie dostępne funkcje umożliwiają ochronę tych użytkowników zdalnych i jakie są różnice poziomu ochrony w przypadku użytkownika w sieci fizycznej lub poza nią. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Proszę szczegółowo opisać, łącznie ze wszystkimi niezbędnymi składnikami, dostępne opcje ochrony użytkowników zdalnych.
- Jeżeli uwzględniono składnik kliencki, jak jest on rozpowszechniany?
- Proszę opisać wymagania dotyczące dostosowania wielkości systemów. Ilu użytkowników można obsługiwać równocześnie?
- Czy funkcja ochrony użytkowników zdalnych jest przezroczysta dla klientów końcowych?
- Proszę opisać jak zasady zabezpieczeń dotyczące użytkowników zdalnych są wdrażane (np. w zasadach firewalla, w oddzielnych zasadach/urządzeniu itd.).
- Proszę wymienić wszystkie funkcje i zabezpieczenia modułów zdalnych (protokół SSL, kontrola aplikacji, system IPS itd.)
- Czy firewall może utrzymywać połączenia użytkowników, aby zapewnić spójne egzekwowanie zasad niezależnie od lokalizacji?
- Jak są obsługiwani użytkownicy korzystający z urządzeń przenośnych? Czy można zapewnić spójne egzekwowanie zasad w przypadku użytkowników w sieciach zewnętrznych i wewnętrznych sieciach bezprzewodowych?
- Czy firewall może rozwiązywać problemy typu BYOD i na przykład umożliwiać bezpieczne korzystanie zarówno z firmowych, jak i spersonalizowanych komputerów przenośnych, telefonów i tabletów?

Zarządzanie

Zarządzanie jest najważniejszym czynnikiem w przypadku wdrażania efektywnych zabezpieczeń sieci. Podczas przejścia do nowego firewalla najważniejszym celem musi być uproszczenie zarządzania zabezpieczeniami, jeżeli jest to możliwe, dzięki dodaniu widoczności i kontroli aplikacji. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Czy oddzielny serwer lub komputer jest wymagany do zarządzania urządzeniami?
- Proszę opisać wszystkie obsługiwane opcje zarządzania: Interfejs wiersza polecenia (CLI)? Przeglądarka? Oprogramowanie klienckie? Serwer centralny?
  - Dla każdej obsługiwanej opcji zarządzania proszę opisać jaki nakład pracy jest wymagany do zmiany metody zarządzania.
- Proszę opisać centralną architekturę zarządzania i opcje wdrażania.
- Jakie dostępne narzędzia do monitorowania, poza przeglądarką logów i raportami, zapewniają przejrzysty obraz aplikacji, użytkowników i zawartości w sieci?
  - Czy narzędzia do monitorowania uwzględniono w konfiguracji podstawowej czy też są udostępniane na podstawie licencji kupowanych/dodawanych oddzielnie?
  - Czy narzędzia do monitorowania są wdrażane w zestawie czy jako oddzielne urządzenie?
- Proszę szczegółowo opisać zasoby i kroki wymagane do uzyskania „pełnego widoku ruchu sieciowego związanego ze wszystkimi aplikacjami".
- Czy wszystkie zasady zabezpieczeń aplikacji, zasady zabezpieczeń firewalla i funkcje zapobiegania zagrożeniom można włączyć w pojedynczej regule w edytorze zasad firewalla?
- Proszę opisać funkcje związane z logami i raportami. Jeżeli są one uwzględnione w zestawie, jaki spadek wydajności powoduje włączenie rejestrowania informacji w logach?
  - Czy pełna analiza logów jest dostępna w zestawie czy też jest udostępniana na podstawie licencji kupowanej/dodawanej oddzielnie lub przy użyciu oddzielnego urządzenia?
- Czy dostępne są narzędzia raportowania z możliwością pełnego dostosowywania pozwalające zrozumieć zasady korzystania z sieci i wykrywać zmiany użycia sieci?
  - Czy są one udostępniane na podstawie licencji kupowanych/dodawanych oddzielnie lub przy użyciu oddzielnego urządzenia?
- Proszę opisać, jak zapewniany jest dostęp związany z zarządzaniem przy dużym natężeniu ruchu sieciowego i obciążeniu urządzenia.
- Proszę opisać zależności między indywidualnym urządzeniem a centralnym zarządzaniem wieloma urządzeniami.
- Proszę opisać różnice w zarządzaniu urządzeniami sprzętowymi i wirtualnymi.

Przepływność

Rzeczywista wydajność jest najważniejszym czynnikiem w przypadku wdrażania zabezpieczeń. Kontrola aplikacji wymaga znacznie dokładniejszej analizy ruchu sieciowego niż w przypadku firewalli blokujących porty, dlatego powoduje znacznie większe zużycie mocy obliczeniowej. Dodanie inspekcji zagrożeń i zasad zabezpieczeń do ruchu sieciowego powoduje tylko zwiększenie obciążenia firewalla. Należy koniecznie ustalić wydajność sieci po włączeniu wszystkich funkcji zabezpieczeń i podczas analizy rzeczywistego ruchu sieciowego. Przygotowując zapytanie ofertowe dotyczące firewalli nowej generacji, należy uwzględnić następujące informacje i pytania.

- Należy sprawdzić, czy produkt jest oparty na oprogramowaniu, serwerze producenta OEM czy urządzeniu specjalistycznym.
- Należy zbadać architekturę sprzętu w celu potwierdzenia odpowiedniej mocy obliczeniowej wymaganej do nieustannej klasyfikacji oraz inspekcji ruchu sieciowego na poziomie aplikacji.
- Proszę opisać ruch sieciowy, dla którego uzyskano publikowane wyniki pomiaru wydajności:
  - Firewall + rejestrowanie informacji w logach
  - Firewall + kontrolowanie aplikacji
  - Firewall + kontrolowanie aplikacji + zapobieganie zagrożeniom
- Jaka jest znamionowa przepustowość dla:
  - Firewall + rejestrowanie informacji w logach
  - Firewall + kontrolowanie aplikacji
  - Firewall + kontrolowanie aplikacji + zapobieganie zagrożeniom

Dodatkowe zalecenia dotyczące zapytań ofertowych (RFP)

W każdej organizacji obowiązują różne wymagania bardziej lub mniej restrykcyjne niż wymagania opisane w tym dokumencie. Przykłady to rozwój firmy, referencje klienta, łatwość wdrożenia oraz obsługa sieci i routingu. Najważniejszym zaleceniem dotyczącym zapytania ofertowego (RFP) jest konsekwentne prowadzenie dostawców, tak aby mogli udowodnić, że proponowane przez nich produkty rzeczywiście oferują deklarowane funkcje.

Zagadnienia związane z wydajnością

Należy koniecznie ustalić wydajność sieci po włączeniu wszystkich funkcji zabezpieczeń i podczas analizy rzeczywistego ruchu sieciowego.

Formalne testy związane z oceną firewalli nowej generacji

Po wybraniu dostawcy lub przygotowaniu „końcowej" listy wybranych dostawców, na podstawie odpowiedzi na zapytanie ofertowe, należy fizycznie ocenić firewall przy użyciu wzorców ruchu sieciowego, obiektów i zasad zgodnych z działalnością biznesową organizacji. W tej sekcji zamieszczono zalecenia dotyczące fizycznej oceny firewalla nowej generacji. Ocena umożliwi ustalenie w rzeczywistym środowisku, jak skutecznie dostawca firewalla uwzględnił najważniejsze wymagania. Poniższe zalecane testy są tylko przykładem wymaganych funkcji firewalla nowej generacji i zostały opisane w celu ułatwienia opracowania szczegółowego planu testów.

Widoczność i kontrolowanie aplikacji

Ta sekcja ma trzy cele. Po pierwsze należy ustalić, że pierwszym zadaniem wykonywanym przez testowane urządzenie (DUT) jest klasyfikacja ruchu sieciowego na podstawie tożsamości aplikacji, a nie portu sieciowego. Po drugie należy ustalić, że testowane urządzenie klasyfikuje aplikacje niezależnie od metody obchodzenia zabezpieczeń, takich jak wymiana portów (port hopping) lub użycie portów niestandardowych, w celu rozszerzenia zakresu dostępności. Po trzecie należy ustalić, że tożsamość aplikacji jest podstawą zasad firewalla, a nie elementem zasad dodatkowych.

Identyfikacja aplikacji

- Należy potwierdzić, czy firewall może identyfikować różne aplikacje. Optymalną metodą wykonania tego zadania jest wdrożenie testowanego urządzenia (DUT) w sieci docelowej w trybie transparentnym, w którym nie będzie ono wpływać na funkcjonowanie sieci.
- Należy zweryfikować, czy testowane urządzenie poprawnie identyfikuje ruch sieciowy związany z aplikacjami, przy użyciu zarówno narzędzi graficznych i podsumowujących, jak i dochodzeniowych.
  - Należy ustalić ilość zasobów administracyjnych wymaganych do wykonania tego zadania.
- Należy ocenić kroki wymagane do wstępnego uaktywnienia mechanizmu identyfikującego aplikacje. Jak szybko użytkownik może skonfigurować zasady i rozpocząć „monitorowanie" ruchu sieciowego związanego z aplikacjami? Czy dodatkowe kroki są wymagane do monitorowania aplikacji stosujących metodę wymiany portów (port hopping) lub korzystających z niestandardowych portów?

Identyfikacja aplikacji stosujących metodę wymiany portów (port hopping) lub korzystających z niestandardowych portów

- Należy zweryfikować, czy firewall może identyfikować i kontrolować aplikacje korzystające z portów innych niż ich porty domyślne. Na przykład protokół SSH na porcie 80 i protokół Telnet na porcie 25.
- Należy potwierdzić, czy firewall może identyfikować aplikacje wykorzystujące znaną aplikację stosującą metodę wymiany portów (port hopping), taką jak Skype, AIM lub jedna z wielu aplikacji P2P.

Tożsamość aplikacji jako podstawa zasad zabezpieczeń firewalla

- Należy potwierdzić, czy podczas tworzenia firewalla aplikacja, a nie port, jest podstawowym elementem.
  - Czy zasady kontroli aplikacji wymagają określenia najpierw reguły dotyczącej portu?
  - Czy moduł kontroli aplikacji jest całkowicie niezależnym edytorem zasad?
- Należy utworzyć zasady akceptujące określone aplikacje i blokujące inne i zweryfikować, czy te aplikacje są kontrolowane zgodnie z oczekiwaniami.
- Czy zasady dotyczące aplikacjach są zgodne z regułą „blokowanie wszystkich pozostałych", na której jest oparty firewall?

Identyfikowanie i kontrolowanie prób obejścia zabezpieczeń

- Należy potwierdzić, czy testowane urządzenie (DUT) może identyfikować i kontrolować grupę aplikacji używanych do obchodzenia zabezpieczeń. Do tej grupy należą aplikacje takie jak zewnętrzne serwery proxy (PHproxy, Kproxy), narzędzia do zdalnego dostępu do komputerów (RDP, LogMeIn!, TeamViewer, GoToMyPC) i szyfrowane tunele niezwiązane z sieciami VPN (Tor, Hamachi, UltraSurf).
- Należy potwierdzić, czy wszystkie aplikacje obchodzące zabezpieczenia są precyzyjnie identyfikowane podczas testu.
- Należy zweryfikować, czy wszystkie aplikacje obchodzące zabezpieczenia mogą być blokowane, nawet wówczas, gdy korzystają z niestandardowego portu.

Identyfikowanie i kontrolowanie aplikacji korzystających z protokołu SSL lub SSH

Coraz większa liczba aplikacji używa szyfrowania SSL i protokołu SSH do alternatywnych celów, dlatego należy ocenić zdolność do identyfikowania i kontrolowania aplikacji tego typu.

- Należy zweryfikować, czy testowane urządzenie (DUT) może identyfikować i deszyfrować aplikacje korzystające z szyfrowania SSL.
- Należy potwierdzić, czy testowane urządzenie (DUT) może identyfikować, deszyfrować i stosować zasady zabezpieczeń w odniesieniu do deszyfrowanych aplikacji.
- Należy sprawdzić, czy deszyfrowana aplikacja „zaakceptowana" przez firewall zostanie ponownie zaszyfrowana i wysłana do oryginalnej lokalizacji docelowej.
- Należy potwierdzić możliwość deszyfrowania oraz inspekcji przychodzącego i wychodzącego ruchu sieciowego związanego z protokołem SSL.
- Należy zweryfikować, czy pakiety protokołu SSH są precyzyjnie identyfikowane niezależnie od portu.
- Należy sprawdzić, czy kontrola protokołu SSH odróżnia przekierowanie portów (lokalne, zdalne, X11) od użycia macierzystego (SCP, SFTP i dostęp do powłoki).

Identyfikowanie i kontrolowanie aplikacji korzystających z tego samego połączenia

Należy ustalić, czy mechanizmy klasyfikowania aplikacji nieustannie monitorują stan aplikacji, sprawdzają zmiany w aplikacji, a przede wszystkim poprawnie klasyfikują zmiany stanu. Wiele „platform" (Google, Facebook, Microsoft) udostępnia różne aplikacje użytkownikom po wstępnym zalogowaniu. Śledzenie tej zmiany stanu aplikacji jest najważniejszym elementem firewalla nowej generacji.

- Podczas korzystania z aplikacji takiej jak WebEx lub SharePoint należy najpierw potwierdzić, czy testowane urządzenie (DUT) identyfikuje początkową aplikację (np. WebEx lub SharePoint).
- Bez wylogowania z aplikacji należy przełączyć się do oddzielnej funkcji (udostępnianie pulpitu WebEx, administracja programu SharePoint, dokumenty programu SharePoint) i sprawdzić, czy ta zmiana stanu jest śledzona, a nowa aplikacja/funkcja jest rzeczywiście poprawnie identyfikowana.
- Należy sprawdzić kontrolę oraz inspekcję zasad w odniesieniu do funkcji aplikacji.

Kontrola funkcji aplikacji

Należy ustalić zdolność testowanego urządzenia (DUT) do identyfikowania i kontrolowania określonych funkcji w aplikacji. Kontrola na poziomie funkcji jest najważniejszym czynnikiem umożliwiającym korzystanie z aplikacji przy zachowaniu pewnej kontroli nad skojarzonymi zagrożeniami dla firmy i systemu zabezpieczeń. Przesyłanie plików jest typowym przykładem, jednak dotyczy to również funkcji administracyjnych, telefonii internetowej (VoIP), publikowania w mediach społecznościowych i prowadzenia rozmowy w aplikacji nadrzędnej.

- Należy potwierdzić, czy testowane urządzenie (DUT) zapewnia widoczność hierarchii aplikacji (zarówno aplikacja podstawowa, jak i dodatkowe funkcje).
- Należy zweryfikować kontrolę funkcji przesyłania plików dzięki identyfikacji i kontroli aplikacji obsługującej tę funkcję.
- Należy potwierdzić zdolność testowanego urządzenia (DUT) do blokowania przesyłania/pobierania plików zależnie od aplikacji i typu plików. Na przykład możliwość blokowania prób przesyłania przez użytkowników dokumentów programu Word przy użyciu internetowej aplikacji poczty sieci Web.

Systematyczne zarządzanie nieznanym ruchem sieciowym

We wszystkich sieciach występuje niewielka ilość nieznanego ruchu, dlatego należy sprawdzić, jak szybko można zidentyfikować ruch tego typu i podjąć odpowiednie działania.

- Należy sprawdzić, czy zapewniona jest widoczność nieznanego ruchu i dostępne są co najmniej następujące informacje:
  - Natężenie ruchu sieciowego
  - Użytkownik i/lub adresy IP
  - Używany port
  - Skojarzona zawartość (plik, zagrożenie itd.)
- Jaka ilość zasobów administracyjnych jest wymagana do badania nieznanego ruchu?
- Czy można konfigurować zasady firewalla (zezwalanie, blokowanie, inspekcja itd.) dla nieznanego ruchu?
- Należy potwierdzić dostępne opcje umożliwiające precyzyjne identyfikowanie i kontrolowanie ruchu sieciowego związanego z nieznanymi aplikacjami.
  - Czy można „zmienić nazwę" ruchu sieciowego?
  - Czy użytkownik może utworzyć niestandardowy mechanizm identyfikacji?
  - Czy dostawca zapewnia niestandardowy mechanizm identyfikacji, a jeżeli tak, to jak szybko?

Ograniczenie obszaru ataku
Aby chronić sieć, należy nie tylko ściśle kontrolować narażenie na zagrożenia, ale również zapewnić niezawodne metody zapobiegania zagrożeniom związanym z akceptowanym ruchem sieciowym aplikacji.

Zapobieganie zagrożeniom

Aby chronić sieć, należy nie tylko ściśle kontrolować narażenie na zagrożenia, ale również zapewnić niezawodną ochronę przed znanymi i nieznanymi zagrożeniami związanymi z akceptowanym ruchem sieciowym aplikacji. Należy sprawdzić zdolność testowanego urządzenia (DUT) do egzekwowania zabezpieczeń w rzeczywistym środowisku, łącznie z nieznanymi zagrożeniami, zagrożeniami związanymi z aplikacjami korzystającymi z niestandardowych portów i ukrytymi przez kompresję, pod warunkiem że spełnione są wymagania przedsiębiorstwa dotyczące wydajności.

- Należy potwierdzić precyzję profilów zapobiegania zagrożeniom — czy są globalne (tylko) czy mogą być konfigurowane indywidualnie zależnie od ruchu sieciowego, zagrożenia, użytkownika itd.
- Należy zweryfikować, czy metody zapobiegania zagrożeniom (system IPS, złośliwe oprogramowanie, filtrowanie zawartości) są spójnie stosowane w odniesieniu do aplikacji (i zagrożeń) korzystających z niestandardowych portów. Oznacza to, że testowane urządzenie (DUT) powinno nie tylko kontrolować aplikacje korzystające z niestandardowych portów, ale również blokować zagrożenia związane z ruchem sieciowym przekazywanym przez te porty.
- Należy zweryfikować, czy testowane urządzenie (DUT) wykrywa złośliwe oprogramowanie i niezatwierdzone pliki nawet wówczas, gdy są skompresowane (np. ZIP lub GZIP).
- Należy ustalić proces identyfikowania i blokowania nieznanego złośliwego oprogramowania.
- Należy weryfikować wydajność testowanego urządzenia (DUT) po włączeniu wszystkich mechanizmów zapobiegania zagrożeniom, aby upewnić się, że ochrona będzie prawidłowo funkcjonować w rzeczywistym środowisku.

Ochrona użytkowników zdalnych

Po pierwsze należy ustalić, czy testowane urządzenie (DUT) może chronić użytkowników zdalnych przy użyciu tych samych zasad, które są stosowane wewnątrz sieci, a po drugie określić ilość zasobów administracyjnych wymaganych do zarządzania i stopień złożoności wdrożenia.

- Należy zweryfikować, czy testowane urządzenie (DUT) może chronić użytkowników zdalnych korzystających z bardziej zaawansowanych technologii niż połączenie SSL VPN lub zwrotne.
- Należy potwierdzić łatwość wdrożenia i zarządzania po utworzeniu grupy użytkowników zdalnych i wdrożeniu zasad testowych.
- Czy testowane urządzenie (DUT) zapewnia zasady zależnie od typu urządzenia?
- Czy testowane urządzenie (DUT) zapewnia ochronę przed złośliwym oprogramowaniem w urządzeniach przenośnych i lukami w systemie operacyjnym tych urządzeń?
- Czy testowane urządzenie (DUT) zapewnia zasady zależnie od typu urządzenia?
- Na zakończenie testu należy monitorować użytkowników zdalnych przy użyciu przeglądarki logów.

Zarządzanie

Należy rozważyć stopień złożoności (liczba oddzielnych modułów sprzętowych) i trudności (liczba kroków, przejrzystość interfejsu użytkownika itd.) zarządzania testowanym urządzeniem (DUT) podczas wykonywania zadań.

- Należy potwierdzić metodologię zarządzania testowanym urządzeniem (DUT) (czy wymagane jest oddzielne urządzenie lub serwer, czy można zarządzać przy użyciu przeglądarki, czy wymagany jest rozbudowany klient)?
- Należy zweryfikować dostępność narzędzi umożliwiających wizualizację wszystkich składników sieci na podstawie podsumowania aplikacji, zagrożeń i adresów URL.
  - Czy logi są przechowywane w centralnej lokalizacji czy w oddzielnych bazach danych na poziomie funkcji (np. firewall, kontrola aplikacji, system IPS)?
  - Należy określić ilość zasobów administracyjnych skojarzonych z analizą logów dla celów związanych z monitorowaniem i prowadzeniem dochodzenia.
- Należy sprawdzić, czy wszystkie zasady zabezpieczeń aplikacji, zasady zabezpieczeń firewalla i funkcje zapobiegania zagrożeniom można włączyć w tym samym edytorze zasad?
  - Czy reguła firewalla dotycząca portów jest tworzona i stosowana przed kontrolą na poziomie aplikacji?
  - Jeżeli używanych jest wiele zasad (np. firewall, kontrola aplikacji, system IPS), czy są dostępne narzędzia do uzgadniania zasad umożliwiające wykrywanie potencjalnych luk?

Wydajność po uruchomieniu usług

Kontrola aplikacji wymaga znacznie większej mocy obliczeniowej niż tradycyjny firewall blokujący porty, dlatego najważniejsze jest sprawdzenie, czy testowane urządzenie (DUT) może funkcjonować prawidłowo podczas identyfikowania i kontrolowania aplikacji.

- Należy sprawdzić, czy testowane urządzenie (DUT) jest oparte na oprogramowaniu, serwerze producenta OEM czy urządzeniu specjalistycznym.
- Jeżeli jest to urządzenie, należy zbadać architekturę sprzętu w celu potwierdzenia odpowiedniej mocy obliczeniowej wymaganej do utrzymania wydajności sieci po uruchomieniu wszystkich usług.
- Należy wykonać test! Należy ocenić rzeczywistą wydajność w środowisku testowym przy użyciu wzorców ruchu sieciowego reprezentatywnego dla docelowego środowiska sieciowego.

Zalecenia dotyczące urządzeń sprzętowych i wirtualnych

Jeżeli docelową lokalizacją wdrożenia jest centrum danych, należy wybrać powyższe testy umożliwiające prawidłowe sprawdzenie funkcji firewalla w formie wirtualnej. W przypadku środowisk wirtualnych należy uwzględnić dodatkowe czynniki:

- Jaki proces jest używany do zarządzania zasadami z uwzględnieniem relacji między instancjami maszyn wirtualnych. Ile kroków jest wymaganych?
- Czy można tworzyć zasady tego samego typu dla urządzeń fizycznych i wirtualnych?

- Czy dokładnie te same funkcje są dostępne w przypadku urządzeń sprzętowych i wirtualnych.
- Należy zweryfikować, czy testowane urządzenie (DUT) może zabezpieczyć cały ruch sieciowy między urządzeniami wirtualnymi na tym samym serwerze wirtualnym.
- Należy zweryfikować, czy testowane urządzenie (DUT) może zapewnić zasady dotyczące aplikacji, użytkowników i zawartości dla danej instancji wirtualnej.
- Należy zweryfikować, czy testowane urządzenie (DUT) może kontynuować egzekwowanie zasad nawet w przypadku migracji maszyny wirtualnej z jednego serwera na drugi.
- Należy potwierdzić i sprawdzić interakcję z systemem zarządzania platformami wirtualizacji.
- Należy potwierdzić i sprawdzić interakcję z systemami automatyzacji i instrumentacji środowiska wirtualnego.

Dodatkowe zalecenia dotyczące oceny

Proces oceny i testowania zabezpieczeń sieci jest zależny od organizacji i w większości wypadków przekracza zakres tego dokumentu. Przykłady to łatwość wdrożenia (tryb pasywnego nasłuchu, tryb transparentny itd.), sieci (warstwa 2, warstwa 3, tryb mieszany) i obsługa routingu (RIP, OSPF, BGP). Zalecaną najlepszą metodą oceny firewalla jest utworzenie określonego zestawu kryteriów i poddanie każdego urządzenia pełnej serii testów, szczegółowe udokumentowanie wyników w sposób umożliwiający podjęcie uzasadnionej ostatecznej decyzji.

Bezpieczne korzystanie z aplikacji dzięki firewallom nowej generacji

Dotychczas zezwolenie pracownikowi na korzystanie z zewnętrznej lub osobistej aplikacji do pracy było wykluczone. Obecnie pracownicy są zawsze w trybie online i nieustannie korzystają z najnowszych aplikacji, które często łączą zastosowania osobiste i służbowe. Zbiorcze blokowanie tych aplikacji oznaczałoby przerwę w działalności firmy.

Informacje zamieszczone w sekcji *10 warunków, które musi spełnić Twój nowy firewall*, potwierdzają, że najlepszą metodą bezpiecznego udostępniania aplikacji jest stosowanie firewalla identyfikującgo aplikacje i korzystającego z tradycyjnego pozytywnego modelu zasad kontroli (firewall), umożliwiającego administratorom wybieranie akceptowanych i odrzucanych aplikacji zależnie od prowadzonej działalności biznesowej. Po skorzystaniu z narzędzi opisanych w tym dokumencie powinno być oczywiste, że bezpieczne udostępnianie aplikacji przy użyciu negatywnego modelu kontroli (podobnego do systemu IPS) jest rozwiązaniem nierealistycznym.

O firmie Palo Alto Networks

Firma Palo Alto Networks® jest wiodącym dostawcą zabezpieczeń sieci nowej generacji. Używając jej nowatorskiej platformy, przedsiębiorstwa, dostawcy usług i jednostki rządowe mogą zabezpieczać swoje sieci i umożliwić bezpieczne korzystanie w tych sieciach z coraz bardziej złożonych i rozpowszechnionych aplikacji, a jednocześnie zapewniać ochronę przez zagrożeniami występującymi w cyberprzestrzeni. Podstawowym składnikiem platformy, opracowanej przez firmę Palo Alto Networks, jest firewall nowej generacji zapewniający widoczność aplikacji, użytkowników i zawartości oraz kontrolę zintegrowaną z firewallem za pośrednictwem opatentowanej architektury sprzętu i oprogramowania. Produkty i usługi firmy Palo Alto Networks są zgodne z wieloma wymaganiami dotyczącymi zabezpieczeń sieci, od centrum danych do granicy sieci, a także rozproszonego przedsiębiorstwa z biurami oddziałowymi i coraz większą liczbą urządzeń przenośnych. Produkty firmy Palo Alto Networks są używane przez ponad 12 500 klientów w ponad 100 krajach.

Więcej informacji znajduje się na stronie www.paloaltonetworks.com.

the network security company™

www.paloaltonetworks.com