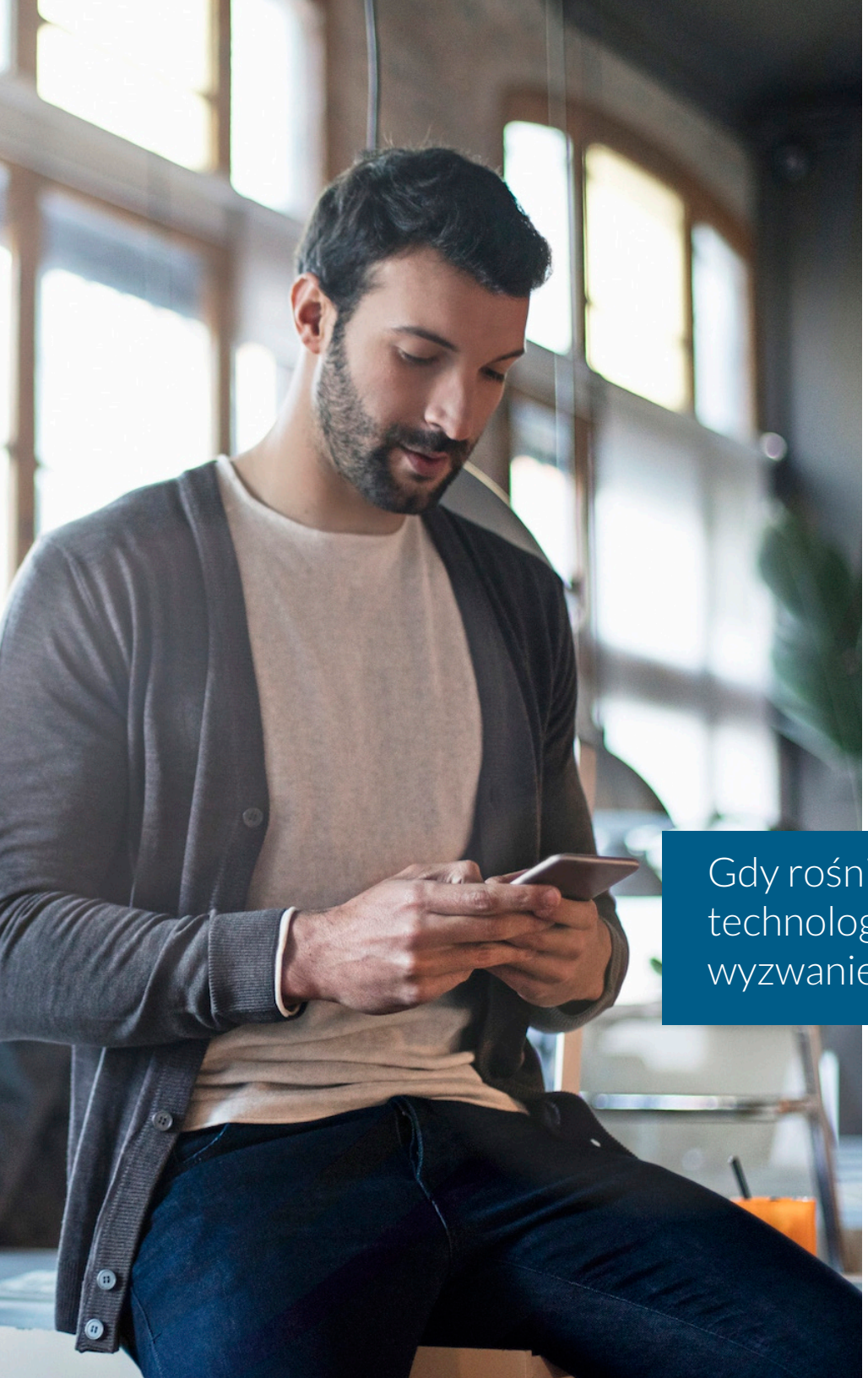
11 SUPER RZECZY KTÓRE POWINIEN ROBIĆ TWÓJ FIREWALL

Rozszerz blokowanie sieciowych zagrożeń o ochronę, zarządzanie i kontrolowanie ruchu aplikacyjnego

SONICWALL

Spis treści

SONICWALL®



Zapory rosną w siłę

Tradycyjne firewalle z mechanizmem stateful packet inspection skupiają się na blokowaniu zagrożeń w sieci, dokonując oceny portów i protokołów wykorzystywanych przez ruch w warstwie sieciowej. Z kolei zapory nowej generacji (NGFW) wykorzystują technikę deep packet inspection do skanowania całej zwartości pakietów, oferując zaawansowane zapobieganie włamaniom, ochronę antymalware, filtrowanie treści i antyspam. Obecnie wiele aplikacji jest dostarczanych przy użyciu tych samych, typowych dla WWW portów i protokołów, takich jak HTTP lub HTTPS. W rezultacie dla tradycyjnych firewalli aplikacje takie stają się niewidoczne Tym samym nie mogą one nadawać priorytetu produktywnemu i bezpiecznemu ruchowi, blokując ten niepożyteczny i potencjalnie niebezpieczny. Z kolei zapory nowej generacji zapewniają wgląd w aplikacje, dostarczając specjalistom sieciowym funkcjonalności, które są dziś krytyczne.

Gdy rośnie popularność przetwarzania w chmurze i technologii Web 2.0, firewalle stoją przed nowym wyzwaniem do pokonania - kontrolą aplikacji.

SONICWALL®

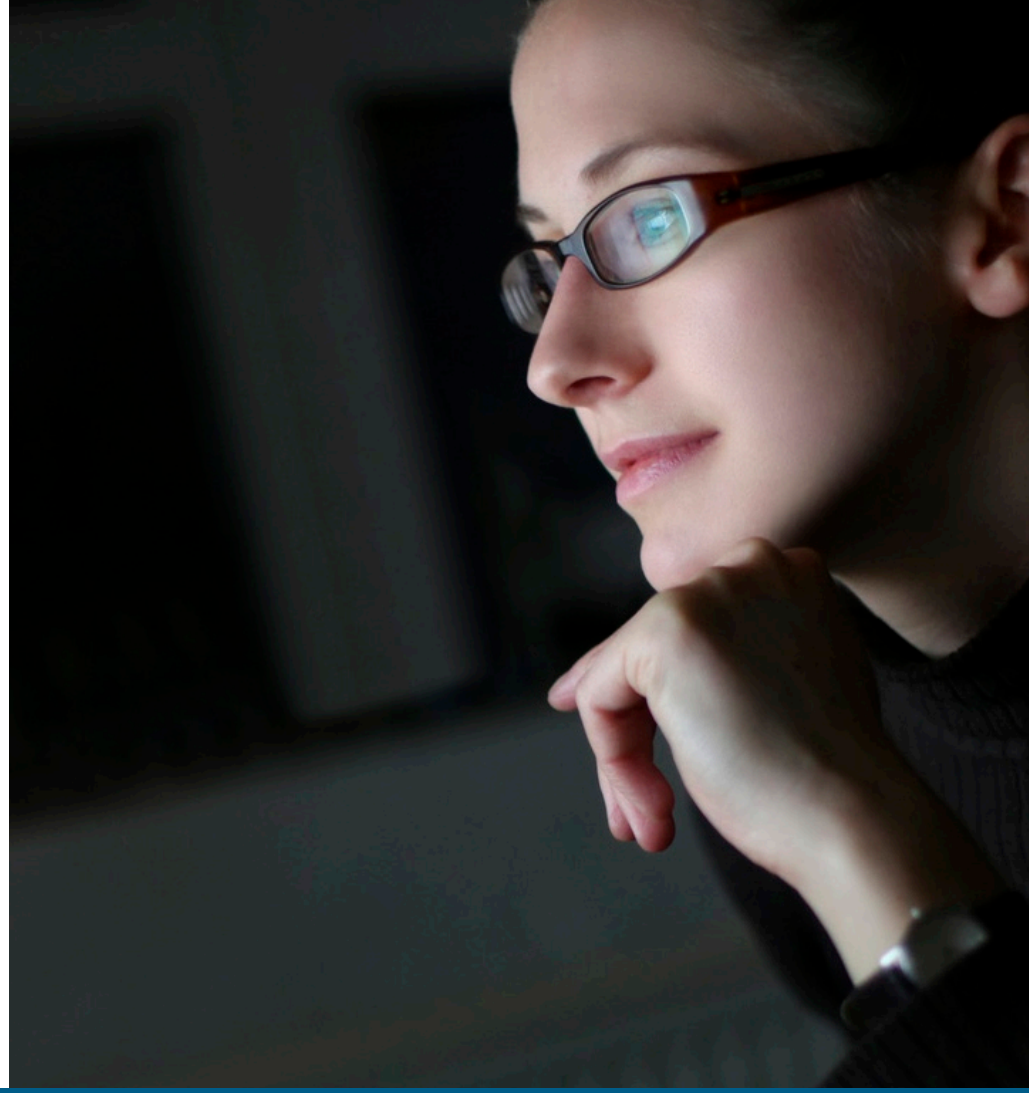
Czym jest SonicWall Application Intelligence and Control?

Firewalle SonicWall identyfikują i kontrolują wszystkie aplikacji używane w sieci. Dzięki rozpoznawaniu aplikacji na podstawie ich unikalnych sygnatur - a nie portów lub protokołów - dodatkowa kontrola umożliwia utrzymywanie zgodności z przepisami i zapobiega wyciekom danych. Cel osiągany jest poprzez wizualizację ruchu aplikacji w celu określenia wzorców użytkowania, a następnie stworzenie granularnych polityk dla: aplikacji, użytkowników (także ich grup) oraz pór dnia i innych zmiennych. W efekcie powstaje elastyczna kontrola, którą można dopasować do wszystkich wymagań sieciowych.

Zapewniaj przepustowość krytycznym i wrażliwym na opóźnienia aplikacjom.

Jak działa SonicWall Application Intelligence and Control?

Wykorzystując obszerną, stale powiększającą się i automatycznie aktualizowaną bazę sygnatur aplikacji, SonicWall identyfikuje aplikacje na podstawie ich „DNA", a nie tylko mało charakterystycznych atrybutów, takich jak port źródłowy, port docelowy lub typ protokołu. Przykładowo, możemy zezwolić na użycie komunikatorów, ale zablokować przesyłanie w nich plików. Możemy umożliwić dostęp do Facebooka, ale już nie do gier na tej platformie. Mechanizmy kontrolne są dostępne także dla całego szyfrowanego ruchu TLS/SSL, który musi być sprawdzany na równi z połączeniami nieszyfrowanymi. Możemy łatwo wizualizować efekt zastosowanych mechanizmów kontroli, precyzyjnie dostosowując wykorzystanie aplikacji i optymalizując przepustowość sieci.



Kontroluj rodzaje aplikacji, poszczególne aplikacje oraz konkretne funkcjonalności w aplikacjach

Super rzecz nr 1:

Kontroluj dozwolone aplikacje w sieci

Chcesz mieć pewność, że wszyscy twoi pracownicy korzystają z najnowszej wersji Internet Explorera. Twoim zadaniem będzie sprawienie, by wszyscy pracownicy uruchamiający IE9 lub IE10 byli automatycznie przekierowywani na stronę pobierania IE11, tracąc dostęp do innych stron internetowych. Masz do wyboru takie rozwiązania:

- Fizyczne, codzienne sprawdzanie każdego systemu pod kątem wersji przeglądarki
- Napisanie własnego skryptu, który automatycznie będzie sprawdzał wersję przeglądarki
- Ustawienie polityki w SonicWall Application Intelligence and Control i... po kłopocie

Utwórz politykę przekierowywania użytkowników IE9 lub IE10 w celu pobrania najnowszej przeglądarki i zablokowania dostępu do Internetu dla IE9 lub IE10:

- Mechanizm Deep Packet Inspection (DPI) szuka atrybutu User Agent = IE 9.0 lub User Agent = IE 10.0 w nagłówku HTTP
- Polityka przekierowuje użytkowników IE9 lub IE10 na stronę pobierania IE11, jednocześnie blokując dla IE9 lub IE10 dostęp do innych stron internetowych

Przed stworzeniem polityki dzięki wizualizacji aplikacji można zobaczyć, jakie przeglądarki są używane.

SONICWALL®

Super rzecz nr 2:

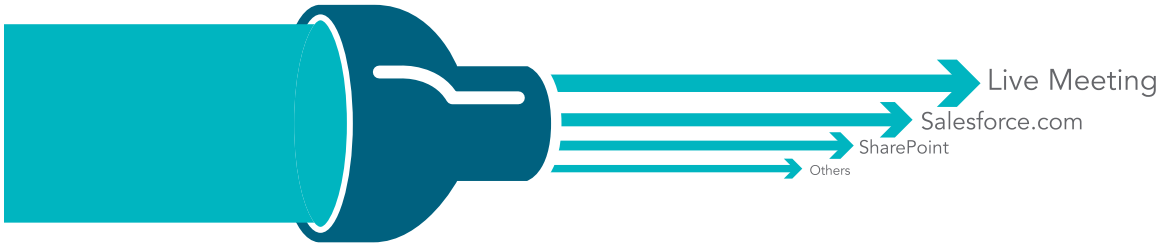
Zarządzaj pasmem dla krytycznych aplikacji

Wiele aplikacji o znaczeniu krytycznym, takich jak Live Meeting, Salesforce.com® i SharePoint®, jest opartych na chmurze lub działa w rozproszonych geograficznie sieciach. Zapewnienie, by aplikacje te miały priorytet nad nieproduktywnym przeglądaniem stron internetowych, zwiększy efektywność biznesu.

Utwórz politykę dającą priorytet aplikacji Live Meeting w przydziale pasma:

1. Mechanizm Deep Packet Inspection szuka sygnatury lub nazwy aplikacji
2. Nadaj aplikacji Live Meeting priorytet w dostępie do pasma

Priorytet dla aplikacji może dotyczyć określonego czasu (np. dla aplikacji sprzedażowych na koniec kwartału).



SONICWALL®

Super rzecz nr 3:

Blokuj aplikacje peer-to-peer

Nieproduktywne aplikacje peer-to-peer (P2P), takie jak BitTorrent, są często używane do pobierania treści chronionych prawem autorskim. Mogą one też szybko zużyć dostępne pasmo i przenosić złośliwe oprogramowanie. Ponieważ stale powstają nowe aplikacje P2P lub pojawiają się modyfikacje już istniejących (np. zmienia się numer wersji), to trudne staje się ręczne blokowanie każdego programu z osobna.

SonicWall stale aktualizuje bazę danych Application Intelligence and Control, dodając nowe aplikacje P2P, gdy tylko się pojawią. Możemy więc po prostu utworzyć jedną politykę, by od razu zablokować wszystkie aplikacje P2P.

Utwórz politykę, by uniemożliwić użycie aplikacji P2P:

- Mechanizm Deep Packet Inspection używa predefiniowanych sygnatur aplikacji P2P z listy sygnatur aplikacji
- Wybierz aplikacje P2P z listy predefiniowanych sygnatur
- Zastosuj politykę do wszystkich użytkowników
- Zablokuj aplikacje P2P przy użyciu ograniczeń pasma i czasu

Lista sygnatur aplikacji

BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
... hundreds more

\+

Lista sygnatur aplikacji

Aktualizacje z SonicWall dostarczone i wprowadzone

=

Lista sygnatur aplikacji

BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
... hundreds more

Cel osiągnięty

- Możesz kontrolować i zarządzać aplikacjami P2P
- Nie marnujesz czasu na uaktualnianie polityk z sygnaturami

SONICWALL

Super rzecz nr 4:

Blokuj nieproduktywne komponenty aplikacji

Serwisy społecznościowe, takie jak Facebook, Instagram czy YouTube, stały się nowymi kanałami komunikacji ludzi i organizacji. Zablokowanie ich wszystkich może przynieść efekt przeciwny do zamierzonego. Jednakże można kontrolować sposób ich wykorzystania w miejscu pracy.

Przykładowo, możemy pozwolić pracownikom marketingu aktualizować profil firmy na Facebooku, ale zabronić im grania na tym serwisie w gry, takie jak Texas HoldEm Poker czy Candy Crush Saga. Dzięki rozwiązaniu Application Intelligence and Control możemy utworzyć politykę dającą dostęp do Facebooka, ale blokującą gry.

Utwórz politykę umożliwiającą dostęp do Facebooka, ale blokującą gry z tego serwisu

1. Wybierz „wszyscy” użytkownicy
2. Wybierz „Gry na Facebooku” jako kategorię
3. Utwórz prostą regułę „Blokuj” dla wszystkich użytkowników

Możesz także udostępnić czat, ale zablokować przesyłanie w nim plików

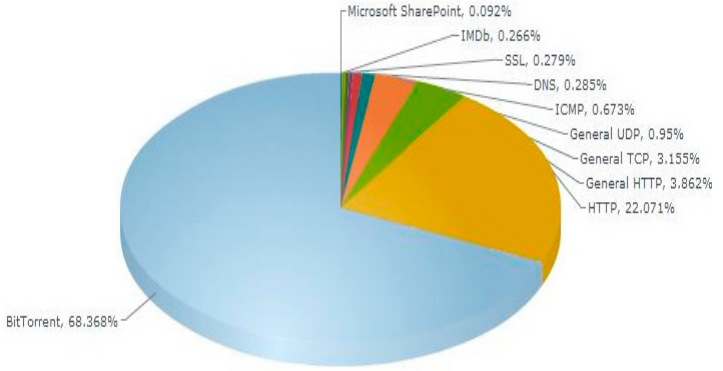
Super rzecz nr 5:

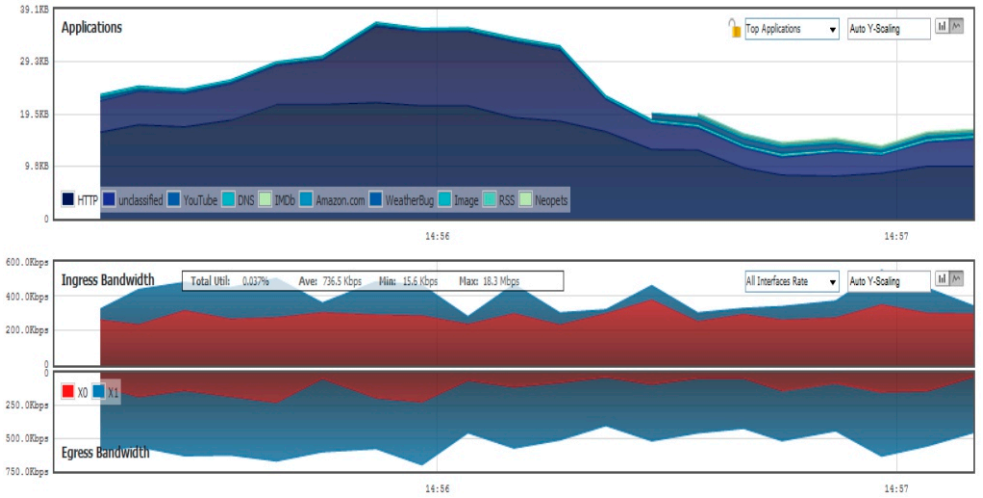
Wizualizuj swój aplikacyjny ruch sieciowy

Co się dzieje w sieci? Kto marnuje pasmo? Dlaczego sieć jest tak wolna? Czy kiedykolwiek zadawaliśmy sobie te pytania? Przy próbie uzyskania na nie odpowiedzi możemy użyć wielu oddzielnych narzędzi, ale proces ten będzie czasochłonny i dostarczy nam wyłącznie informacje po fakcie. Dzięki dokonywanej w czasie rzeczywistym wizualizacji SonicWall możemy natychmiast dostać odpowiedź na te pytania, szybko zdiagnozować problemy, wykryć wykorzystanie sieci niezgodne ze standardami, stworzyć odpowiednie polityki i od razu sprawdzić ich skuteczność.

Zobacz cały ruch w czasie rzeczywistym dzięki logom usługi Application Flow Monitor:

1. Oglądaj wykresy dla całego ruchu aplikacji w czasie rzeczywistym
2. Oglądaj wykresy pasma ingress/egress w czasie rzeczywistym
3. Oglądaj wykresy odwiedzanych stron internetowych i wszystkich aktywności użytkowników w czasie rzeczywistym
4. Stwórz własne filtry, by śledzić najistotniejsze informacje





Wizualizacja daje administratorom natychmiastowy wgląd w przepływy ruchu sieciowego.

SONICWALL

Super rzecz nr 6:

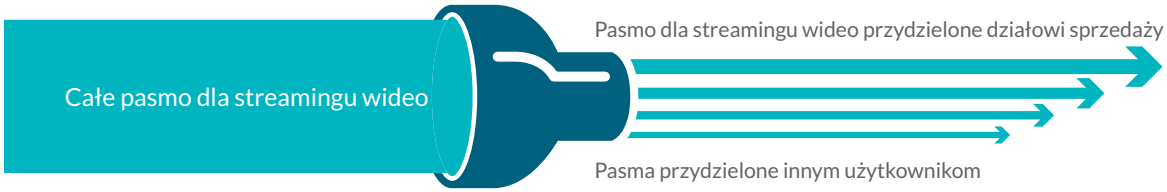
Zarządzaj pasmem dla grupy użytkowników

Co zrobić, jeśli prezes skarży się, że na kanale wideo z wiadomościami biznesowymi, który chce oglądać codziennie rano, firmy zacinają się i nie są poprawnie odtwarzane? Po dochodzeniu ustalamy, że winna jest polityka zarządzania pasmem w całej firmie, którą zaimplementowaliśmy dla wszystkich. Moglibyśmy złagodzić obejmujące wszystkich ograniczenia przepustowości, ale jest lepszy sposób: zarządzanie pasmem oparte na grupach.

Utwórz politykę, która wyłączy zarząd z zarządzania pasmem dla strumieniowych transmisji wideo:

1. Wybierz grupę zarządu, zaimportowaną z serwera LDAP
2. Mechanizm Deep Packet Inspection używa predefiniowanych sygnatur aplikacji streamingu wideo z listy sygnatur aplikacji
3. Ustaw ograniczenia dla ruchu z tym nagłówkiem

Wiele firm odkryło, że pracownicy są bardziej zadowoleni, jeśli mają pełny dostęp do sieci, nawet, jeśli oznacza to dla nich mniejszą przepustowość w dostępie do nieproduktywnych stron



SONICWALL

Super rzecz nr 7:

Blokuj ataki ransomware i włamania

Bezpieczeństwo sieci musi znajdować się w centrum uwagi każdego administratora IT. Możliwość blokowania ataków, takich jak ransomware, innych zagrożeń związanych ze złośliwym oprogramowaniem oraz prób włamań, ogranicza poziom ryzyka w organizacji i zapobiega marnowaniu cennych zasobów. Usługi bezpieczeństwa, dostarczane przez wysoko wydajne i cechujące się ultra niskim opóźnieniem firewalle nowej generacji SonicWall, są w stanie blokować miliony znanych i nieznanych zagrożeń zanim dostaną się do sieci i staną problemem dla organizacji. Rozszerzająca możliwości zapory usługa SonicWall Capture wykrywa nieznane ataki (w tym zero-day) i zapobiega im, wykorzystując oparty na chmurze, wielosilnikowy mechanizm sandboxingu.

Blokuj ataki malware oraz intruzów, zanim dostaną się do twojej sieci!

SONICWALL®

Super rzecz nr 8:

Identyfikuj połączenia według państw

Czy połączenie z adresem IP w obcym kraju z naszego lokalnego biura lub oddziału to niegroźna komunikacja kogoś przeglądającego Internet, czy może stoi za tym aktywność botnetu? Możemy wykorzystać identyfikację ruchu GeoIP w celu weryfikowania i kontrolowania ruchu sieciowego kierowanego do określonych krajów lub z nich pochodzącego, w celu ochrony przed atakami ze znanych źródeł zagrożeń lub podejrzanych lokalizacji oraz badania podejrzanego ruchu wychodzącego z sieci.

Przeglądaj połączenia według krajów i stwórz na tej podstawie odpowiednie filtry:

1. Sprawdź, które aplikacje łączą się z adresami IP w innych krajach
2. Zobacz, którzy użytkownicy i które komputery łączą się z adresami IP innych krajów
3. Utwórz filtry, aby ograniczyć ruch do określonych krajów, z użyciem listy wykluczeń

Gdy znasz już odpowiedź, na czym polega problem, możesz przeprowadzić rozmowę z użytkownikiem, sprawdzić komputer łączący się z wrogim adresem IP lub włączyć narzędzie do przechwytywania pakietów na zaporze, aby dokładnie przeanalizować, co się dzieje z tym połączeniem. Korzystając z identyfikacji ruchu SonicWall GeoIP, można wykrywać i rozwiązywać problemy, z których moglibyśmy nie zdawać sobie sprawy.

Super rzecz nr 9:

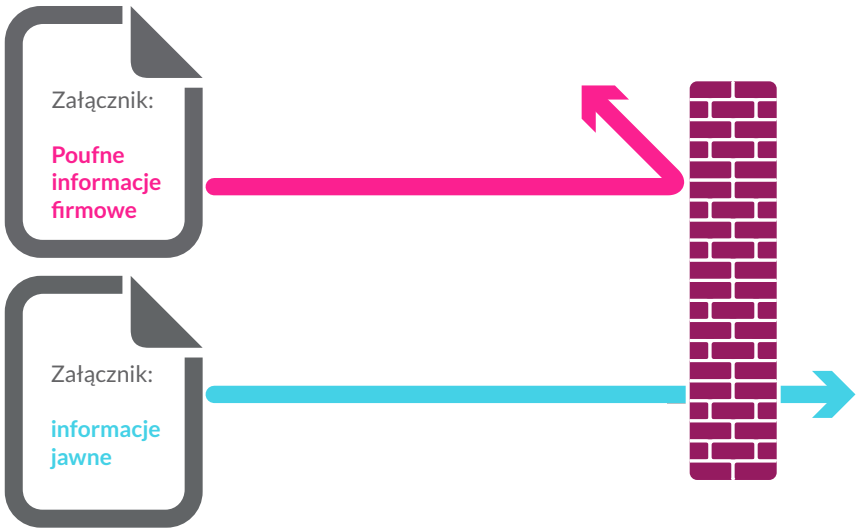
Zapobiegaj wyciekom informacji przez e-mail

Są firmy, w których wychodzące wiadomości e-mail nie przechodzą przez system zabezpieczeń poczty albo nie jest sprawdzana zawartość załączników. W obu przypadkach pliki zawierające „poufne informacje firmowe” mogą łatwo opuścić organizację. Ponieważ wychodzący ruch sieciowy przechodzi przez firewall, można wykryć i zablokować takie „dane w ruchu”.

Utwórz politykę blokowania załączników do wiadomości e-mail, zawierających znak wodny „poufne informacje firmowe”:

Mechanizm Deep Packet Inspection przeszukuje:

1. Zawartość wiadomości e-mail = “poufne informacje firmowe” oraz
2. Zawartość wiadomości e-mail = “zastrzeżone informacje firmowe ” oraz
3. Zawartość wiadomości e-mail = “zastrzeżone informacje prywatne” itp.



SONICWALL®

Super rzecz nr 10:

Zapobiegaj wyciekom informacji przez web mail

Załóżmy nawet, że używana w organizacji ochrona antyspamowa może wykryć i zablokować wiadomość zawierającą „poufne informacje firmowe”, wysyłaną zwykłą pocztą e-mail. A co z przypadkiem, gdy pracownik wysyłający takie dane korzysta z usługi poczty internetowej, takiej jak Gmail® czy Yahoo®?

Utwórz politykę blokującą załączniki „poufne informacje firmowe” w ruchu webowym:

1. Mechanizm Deep Packet Inspection szuka znaku wodnego „poufne informacje firmowe” na plikach przesyłanych przez http lub https

2. Blokuj wiadomość i zawiadamiaj nadawcę, że są to „poufne informacje firmowe”

GO

Od: goodguy@your_company.com
Do: goodguy@partner.com
Temat: Zatwierdzenie wykazu czasu pracy
Zatwierdzam wykaz twojego czasu pracy w tym tygodniu

STOP

Od: badguy@your_company.com
Do: badguy@competitor.com
Temat: Harmonogram projektu
Przesyłam harmonogram projektu
09 styczeń – Release 7.0
Ten dokument to **Poufne informacje firmowe**

Ten sam mechanizm może być zastosowany do treści na FTP.

Super rzecz nr 11:

Zarządzaj pasmem dla streamingu audio i wideo

Dostęp do strumieniowego wideo w serwisach, takich jak YouTube, czasami się przydaje, ale najczęściej jest marnowaniem zasobów. Rozwiązaniem może być blokowanie tego rodzaju serwisów, ale preferowanym podejściem jest ograniczenie całkowitej przepustowości streamingu wideo, niezależnie od tego, skąd pochodzi. Dotyczy to również streamingu audio - z internetowych stacji radiowych i serwisów muzycznych, w rodzaju Spotify i Apple Music. Ruch tego typu niekoniecznie jest związany ze znanymi serwisami internetowymi, bo jego źródłem mogą być także blogi. Dlatego celem jest zidentyfikowanie rodzaju ruchu, a nie jego pochodzenia. W tym procesie świetnie sprawdza się mechanizm Deep Packet Inspection.

Utwórz politykę ograniczającą przesyłanie strumieniowego wideo i audio przy użyciu predefiniowanej listy sygnatur:

- Wybierz Streaming Wideo i Streaming Audio jako kategorie aplikacji
- Ustal przepustowość, jaką chcesz przypisać do tej kategorii aplikacji (np. 10%)
- Utwórz regułę, która wymusza, by streaming wideo i audio zużywał maksymalnie 10% dostępnej dla wszystkich przepustowości (ewentualnie możesz wyłączyć z niej pewne grupy, takie jak np. „szkolenia”)
- Opcjonalnie zastosuj ustawienia, by reguła działała w godzinach pracy, ale nie w porze lunchu lub po 18:00.
- Potwierdź skuteczność nowej polityki dzięki wizualizacji w czasie rzeczywistym, logując się do usługi Application Flow Monitor

SONICWALL®

Jeśli wszystko dodasz…

Wysoko wydajna platforma

+ Mechanizm Deep Packet Inspection

+ Ochrona przed włamaniami

+ Inteligencja, kontrola i wizualizacja aplikacji

SonicWall Next-Generation Firewalls

Bezpieczeństwo, wydajność i kontrola

SONICWALL®

O firmie

SonicWall od ponad 25 lat zapobiega cyberprzestępstwom, broniąc małe i średnie przedsiębiorstwa oraz korporacje na całym świecie. Połączony potencjał produktów i partnerów tworzy ochronę w czasie rzeczywistym, dostosowaną do indywidualnych potrzeb ponad 500 tys. firm z przeszło 150 krajów. Z SonicWall można bez obaw rozwijać swój biznes.

SonicWall, Inc.
5455 Great America Parkway
Santa Clara, CA 9505454
Więcej informacji można znaleźć na naszej stronie internetowej.
www.sonicwall.com