FORTINET

Bewertungsbericht zu Cyber-Bedrohungen

Wichtige Statistiken

Dieses Dokument enthält die Ergebnisse einer kürzlich durchgeführten Analyse Ihrer Infrastruktur.
Das Dokument stellt eine Zusammenfassung dieser Ergebnisse dar und bietet eine Reihe von Empfehlungen zu deren Handhabung. Die Analyse basiert auf Daten, die mithilfe der folgenden Merkmale erhoben wurden:

Unternehmensdetails

Unternehmensname: Fortinet

Standort:

Branche: Consulting

Unternehmensgröße: 25-99 employees

Testdetails

Test-Startdatum: Jun 6, 2016

Testdauer: 2 Tag(e)

FortiGate-Modell: FG-300D

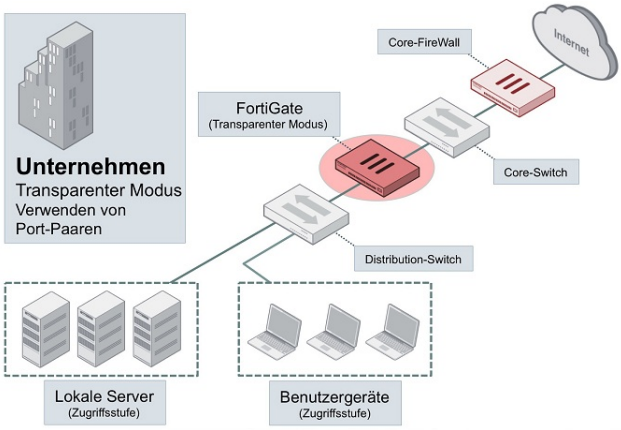
FortiOS-Firmware: FortiOS 5.2.6

Analysiertes Netzwerk: Network Segment

Aktivierte Funktionen: Antivirus, App Control, IPS, Traffic, Web

Implementierung und Methodologie

Ihr Netzwerk wurde mit FG-300D im Transparent Mode (Port Pair)-Modus überwacht. Dies ist ein nichtinvasiver Weg zum Abfangen des Datenverkehrs in Ihrem Netzwerk.



Für die Bewertung wurde die Netzwerkaktivität innerhalb Ihrer Infrastruktur überwacht. Während Datenverkehrprotokolle einen Großteil der in Ihrem Netzwerk übermittelten Sitzungsinformationen protokollieren, ermöglicht die FortiGate-Plattform eine tiefergreifende Überwachung der Sicherheitsprotokollierung wie etwa IPS, Antivirus, Web und Applikationskontrolle. Diese Bewertung wurde anhand von telemetrischen Daten aus allen Protokolltypen erstellt und bietet einen Überblick über Ihre Netzwerkaktivitäten. Zusammen mit FortiAnalyzer kann die FortiGate-Plattform zusätzliche Funktionen wie die Ereignisverwaltung (z. B. Warnmeldungen), FortiView-Analysen (z. B. Untersuchungen bestimmter Benutzeraktivitäten) und Berichterstattungen bereitstellen.

Zusammenfassung

Erkannte IPS-Angriffe: 26,067
Erkannte Malware/Botnets: 1
Stark risikobehaftete Anwendungen: 0
Erkannte infizierte Websites: 0

Im letzten Jahr wurden über 2.100 Unternehmen infolge von mangelhaften internen Sicherheitspraktiken und herstellerseitiger Content Security gehackt. Unternehmen entstehen durch Sicherheitsverletzungen Kosten von im Schnitt 3,5 Millionen USD. Dabei gibt es einen jährlichen Anstieg um 15 %. Unbefugte Zugriffe, Malware/Botnets und Schadprogramme stellen zusammen ein massives Risiko für Ihr Unternehmensnetzwerk dar und ermöglichen Angreifern den Zugriff auf Ihre sensibelsten Dateien und Datenbankinformationen. FortiGuard Labs verringert diese Risiken durch preisgekrönte Content Security. Unabhängige Stellen wie NSS Labs, VB 100 und AV Comparatives bewerten die Lösung wiederholt als marktführend.

Erkannte Anwendungen: 34
Top-Anwendung: Google.Ads
Top-Anwendungskategorie: Network.Service
Besuchte Websites: 96
Top-Website: www.heise.de
Top-Webkategorie: Information Technology

Anwendungsnutzung und Surfverhalten können auf eine ineffiziente Verwendung von Unternehmensressourcen hinweisen und zeigen, dass die Nutzungsrichtlinien des Unternehmens unzureichend durchgesetzt werden. Die meisten Unternehmen tolerieren die private Nutzung von Unternehmensressourcen. Dabei bestehen jedoch auch kritische Grauzonen. Hierzu zählen Proxy-Umgehungs- bzw. Peer-to-Peer-Anwendungen, unangemessene Surfaktivitäten, Phishing-Websites und potenziell illegale Aktivitäten. All dies kann Ihr Unternehmen Haftungsrisiken und potenziellen Schäden aussetzen. Mit über 5800 Applikationskontrollregeln und 250 Millionen kategorisierten Webseiten stellt FortiGuard Labs die erforderlichen Telemetriedaten bereit, mit denen FortiOS einen reibungslosen Geschäftsbetrieb gewährleistet.

Gesamte Bandbreite: 242.51 MB
Top-Host nach Bandbreite: 192.168.0.175
Host mit höchster Sitzungsanzahl: 192.168.0.175
Durchschnittliche Protokollrate/Sek.: 0.25

Die Leistungseffektivität wird bei Sicherheitsgeräten oft unterschätzt. Firewalls müssen mit den Geschwindigkeiten moderner Switches Schritt halten. Einer aktuellen Infonetics-Umfrage zufolge denken 77 % der Entscheidungsträger in Großunternehmen, dass sie ihre Netzwerksicherheitsleistung (Gesamtdurchsatz über 100 Gbit/s) im kommenden Jahr aufrüsten müssen. FortiGate-Plattformen nutzen FortiASICs zur Beschleunigung rechenintensiver Funktionen wie Paketweiterleitung und Mustervergleich. Diese Auslagerung führt gegenüber Konkurrenzlösungen oft zu einer fünf- bis zehnfachen Leistungssteigerung.

Empfohlene Maßnahmen

Erkannte Angriffe auf Anwendungsschwachstellen (3)

Anwendungsschwachstellen (oder IPS-Angriffe) dienen als Zugangspunkte, über die Angreifer die Sicherheitsinfrastruktur umgehen und in Ihre Organisation eindringen. Diese Schwachstellen entstehen häufig durch nicht durchgeführte Updates oder fehlendes Patch-Management. Um Ihre Organisation vor diesen Angriffen zu schützen, ist auf nicht gepatchte Hosts zu achten.

Erkannte Malware (1)

Malware kann in Form von Viren, Trojanern, Spyware/Adware usw. auftreten. Erkannte Malware-Instanzen, die sich im Netzwerk ausbreiten, sind u. U. auch ein Anzeichen für einen innerbetrieblichen und vermutlich unbeabsichtigten Bedrohungsvektor. Die Verwendung von Signaturen in Verbindung mit Verhaltensanalysen verhindert in der Regel die Ausführung von Malware und damit einhergehenden schädlichen Aktivitäten in Ihrem Netzwerk. Indem Sie den Schutz Ihres Netzwerks mit APT-/Sandboxing-Technologie (z. B. FortiSandbox) erhöhen, können Sie auch die Ausbreitung von bis dato unbekannter Malware (Zero-Day-Bedrohungen) in Ihrem Netzwerk verhindern.

Botnet-Infektionen (0)

Mit Botnets bzw. Bots können Denial-of-Service-Angriffe (DoS) gestartet werden. Sie ermöglichen es, Spam, Spyware und Adware zu verteilen, schädlichen Code zu verbreiten und vertrauliche Informationen abzufangen. Dies hat mitunter signifikante finanzielle und rechtliche Folgen. Botnet-Infektionen müssen ernst genommen und sofort behoben werden. Es ist wichtig, mit Botnet infizierte Computer zu identifizieren und mit Antivirus-Software zu bereinigen. Mit FortiClient von Fortinet können Sie Botnets ermitteln und von den infizierten Hosts entfernen.

Erkannte infizierte Websites (0)

Infizierte Websites hosten Software/Malware, die dazu dient verdeckt Informationen zu sammeln, den Hostcomputer zu beschädigen oder das Zielgerät anderweitig ohne Zustimmung des Benutzers zu manipulieren. Der Besuch einer infizierten Website ist oft Ausgangspunkt der Bedrohungskette. Der beste Schutz ist, infizierte Websites zu blockieren und/oder Mitarbeiter anzuweisen, keine unbekannten Websites zu besuchen und keine darauf angebotene Software zu installieren.

Erkannte Phishing-Websites (0)

Phishing-Websites ähneln in ihrer Schädlichkeit infizierten Websites. Sie emulieren die Webseiten legitimer Websites, um persönliche oder private Daten (Benutzernamen, Passwörter usw.) von Endbenutzern zu sammeln. Links zu Phishing-Websites werden oft in Spam-Mails an Ihre Mitarbeiter gesendet. Die meisten Phishing-Angriffe vermeiden Sie, indem E-Mails, in denen nach persönlichen Daten gefragt wird, mit Skepsis betrachtet werden. Die Gültigkeit derartiger Links können Sie ermitteln, indem Sie den Mauszeiger darüber bewegen.

Erkannte Proxy-Anwendungen (0)

Diese dienen dazu, vorhandene Sicherheitsmaßnahmen (bewusst) zu umgehen. Benutzer können z. B. die Firewall umgehen, indem sie externe Kommunikationen tarnen oder verschlüsseln. Dies erfolgt in den meisten Fällen vorsätzlich und verstößt gegen die Nutzungsrichtlinien des Unternehmens.

Erkannte Fernzugriffsanwendungen (0)

Fernzugriffsanwendungen werden oft verwendet, um entfernt auf interne Hosts zuzugreifen. Damit kann die NAT umgangen oder ein sekundärer Zugangspfad bereitgestellt werden. Im Extremfall werden der Datenabschöpfung sowie der Unternehmensspionage durch den Fernzugriff Tür und Tor geöffnet. Der Fernzugriff kann oft uneingeschränkt genutzt werden, weshalb unternehmensinterne Nutzungsänderungen eingeführt werden sollten.

P2P- und Filesharing-Anwendungen (0)

Diese können zur Umgehung bestehender Inhaltskontrollen dienen. Sie ermöglichen unautorisierte Datenübertragungen und verstoßen gegen Datenrichtlinien. Die Implementierung von Richtlinien für diese Anwendungen ist daher wichtig.

Sicherheit und Bedrohungsabwehr

Stark risikobehaftete Anwendungen

Das FortiGuard-Forschungsteam weist Anwendungen basierend auf ihren Verhaltensmerkmalen eine Risikobewertung zwischen 1 und 5 zu. Administratoren können dadurch stark risikobehaftete Anwendungen schnell identifizieren und bessere Entscheidungen bezüglich der Applikationskontrollrichtlinie treffen. Die folgenden Anwendungen wurden mit einer Risikobewertung von 4 oder höher eingestuft.

Stark risikobehaftete Anwendungen

No matching log data for this report

Abbildung 1: Anwendungen mit dem höchsten Risiko, sortiert nach Risiko und Sitzungen

Anwendungsschwachstellen-Exploits

Anwendungsschwachstellen können ausgenutzt werden und die Sicherheit Ihres Netzwerks gefährden. Das FortiGuard-Forschungsteam analysiert diese Schwachstellen und entwickelt anschließend Signaturen zu deren Erkennung. Aktuell bedient sich FortiGuard einer Datenbank mit über 5800 bekannten Anwendungsbedrohungen, um Angriffe auf herkömmliche Firewall-Systeme abzuwehren. Weitere Informationen zu Anwendungsschwachstellen erhalten Sie auf der Website von FortiGuard unter http://www.fortiguard.com/intrusion.

Die wichtigsten erkannten Anwendungsschwachstellen-Exploits

#	Schwere	Bedrohungsname	Typ	Opfer	Quelle	Anzahl
1	2	TCP.Data.On.SYN	Permission/Priviledge/Access Control	1	1	7
2	1	DNS.Invalid.OPcode	Anomaly	25	1	26,056
3	1	Eicar.Virus.Test.File	Anomaly	1	1	4

Abbildung 2: Die wichtigsten identifizierten Schwachstellen, sortiert nach Schwere und Anzahl

Malware, Botnets und Spyware/Adware

Für die Malware-Verbreitung stehen Cyberkriminellen zahlreiche Kanäle zur Verfügung. Bei den gängigsten Methoden werden Benutzer motiviert, einen infizierten E-Mail-Anhang zu öffnen, eine infizierte Datei herunterzuladen oder auf einen Link zu einer infizierten Website zu klicken. Fortinet hat im Rahmen der Sicherheitsbewertung eine Reihe von Malware- und Botnet-Ereignisse identifiziert. Diese deuten darauf hin, dass schädliche Dateien heruntergeladen oder Websites mit Botnet-Befehlen und -Kontrollfunktionen aufgerufen wurden.

Die wichtigsten erkannten Fälle von Malware, Botnets und Spyware/Adware

#	Malware-Name	Typ	Anwendungen	Opfer	Quelle	Anzahl
1	EICAR_TEST_FILE	Virus	HTTP	1	1	3

Abbildung 3: Häufig erkannte Arten von Malware, Botnets, Spyware und Adware

Gefährdete Geräte und Hosts

Basierend auf den unterschiedlichen Arten von Aktivitäten eines individuellen Hosts können wir die Vertrauenswürdigkeit jedes einzelnen Clients bewerten. Diese Client-Reputation basiert auf Schlüsselfaktoren wie aufgerufene Websites sowie genutzten Anwendungen und eingehenden/ausgehenden Zielen. Schließlich können wir eine Gesamtbedrohungswertung erstellen, indem wir uns die gesamten Aktivitäten jedes Hosts ansehen.

Die gefährdetsten Geräte und Hosts

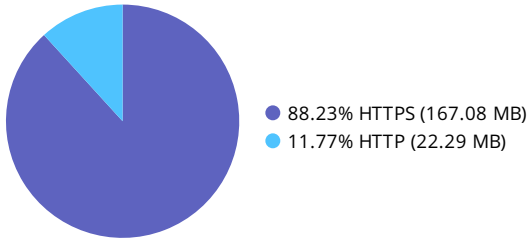
#	Geräte	Bewertungen
1	FG60DP4615001758	185

Abbildung 4: Diese Geräte sollten auf Malware und IPS-Anfälligkeit geprüft werden.

Verschlüsselter Webverkehr

Hinsichtlich der Sicherheit ist es wichtig, zu visualisieren, welcher Anteil Ihres webbasierten Datenverkehrs verschlüsselt ist. Verschlüsselter Datenverkehr stellt Unternehmen vor eine ernsthafte Herausforderung, wenn sie vermeiden möchten, dass diese Anwendungen für schädliche Zwecke wie etwa Datenabschöpfungen verwendet werden. Im Idealfall sollte Ihre Firewall verschlüsselten Datenverkehr bei hohen Geschwindigkeiten inspizieren können. Aus diesem Grund sind die Leistung und die Hardware-/ASIC-Auslagerung bei der Bewertung einer Firewall ausschlaggebend.

Verhältnis des HTTPS-/HTTP-Datenverkehrs



Top-Ursprungsländer

Anhand des Datenverkehrs von der IP-Quelle können wir das Ursprungsland einer jeweiligen Anforderung ermitteln. Bestimmte Botnets, Befehls- und Kontrollfunktionen und sogar der Fernzugriff können sitzungslastig sein und auf gezielte Angriffe oder dauerhafte Bedrohungen durch Nationalstaaten hindeuten. Dieses Diagramm zeigt den landesspezifischen Datenverkehr. Die Aktivitäten von bestimmten Ursprungsnationen können anormal sein und eine eingehendere Untersuchung rechtfertigen.

Top-Ursprungsländer

#	Land	Bandbreite
1	United States	48 B

Abbildung 5: Bei Aktivitäten aus diesen Ländern sollten die erwarteten Datenverkehrsquellen überprüft werden.

Benutzerproduktivität

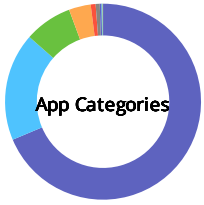
Anwendungsnutzung

Das FortiGuard-Forschungsteam unterteilt Anwendungen basierend auf ihren Verhaltensmerkmalen, der zugrundeliegenden Technologien sowie entsprechenden Eigenschaften der Datenverkehrstransaktionen in unterschiedliche Kategorien. Dies erleichtert die Anwendungssteuerung. FortiGuard verfügt über Tausende von Anwendungssensoren und kann Anwendungen zudem eingehend untersuchen. IT-Manager profitieren beispielsweise von einer einzigartigen Transparenz hinsichtlich der an die Cloud gesendeten Dateien oder der Titel gestreamter Videos.

Details zu Anwendungskategorien erhalten Sie unter http://www.fortiguard.com/encyclopedia/application

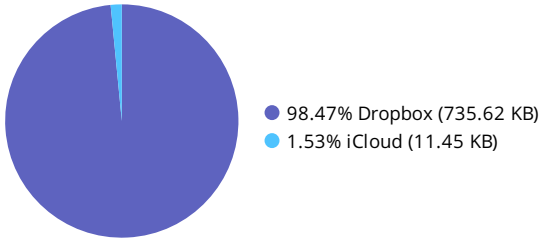
Anwendungskategorien

Network.Service	68.66%
Web.Others	17.81%
Collaboration	7.90%
General.Interest	3.61%
Cloud.IT	0.81%
Social.Media	0.67%
Storage.Backup	0.30%
Video/Audio	0.15%
Business	0.06%
Update	0.03%



Mit der zunehmenden Verbreitung von Cloud Computing sind Unternehmen hinsichtlich der Installation und Verwaltung ihrer Infrastruktur verstärkt von Dritten abhängig. Dies bedeutet jedoch, dass Unternehmensinformationen nur so sicher sind, wie die Sicherheitslösungen des Cloud-Anbieters. Zudem entsteht durch das Cloud Computing häufig eine Redundanz (wenn Services bereits intern verfügbar sind), und die Kosten steigen (bei einer unsachgemäßen Überwachung).

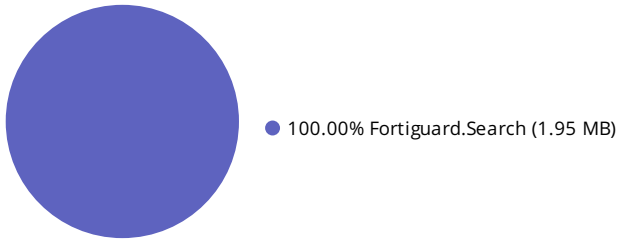
Cloud-Nutzung (SaaS)



IT-Manager sind sich häufig der Menge der innerhalb ihrer Organisation verwendeten Cloud-Services gar nicht bewusst. Diese Anwendungen sollten eigentlich die Benutzerfreundlichkeit erhöhen, werden jedoch mitunter genutzt, um die vorhandene Unternehmensinfrastruktur zu umgehen oder sogar zu ersetzen. Ein möglicher Nebeneffekt ist, dass Ihre sensiblen Unternehmensinformationen in die Cloud gelangen. Bei einem Angriff auf die Sicherheitsinfrastruktur des Cloud-Anbieters könnten Ihre Daten folglich offengelegt werden.

Cloud-Nutzung (IaaS)

Es werden häufig IaaS-Plattformen (Infrastructure-as-a-Service) genutzt. Dies kann hilfreich sein, wenn Computing-Ressourcen begrenzt sind oder speziellen Anforderungen unterliegen. Das effektive Outsourcing Ihrer Infrastruktur muss dabei gründlich reguliert werden, um einen Missbrauch zu vermeiden. Die gelegentliche Prüfung von IaaS-Anwendungen ist nicht nur aus Sicherheitsgründen von Vorteil, sondern kann auch die Betriebskosten für Pay-per-Use-Modelle oder wiederkehrende Abonnementgebühren minimieren.



Unterteilung der Anwendungskategorien

Anwendungsunterkategorien können wertvolle Einblicke in die Betriebseffizienz Ihres Unternehmensnetzwerks bieten. Bestimmte Anwendungstypen (wie P2P- oder Spielanwendungen) sind in Unternehmensumgebungen oft nicht förderlich und lassen sich blockieren oder einschränken. Andere Anwendungen (wie etwa Video-/Audio-Streaming oder Social-Media-Anwendungen) können sowohl privat als auch geschäftlich genutzt und entsprechend gehandhabt werden. Diese Diagramme veranschaulichen Anwendungskategorien, sortiert nach der während des Analysezeitraums genutzten Bandbreite.

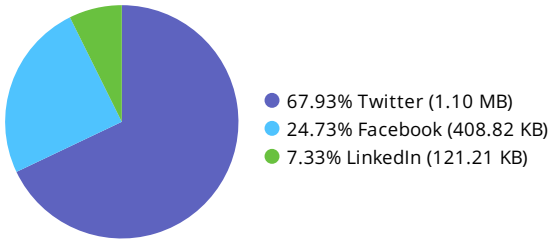
Fernzugriffsanwendungen

No matching log data for this report

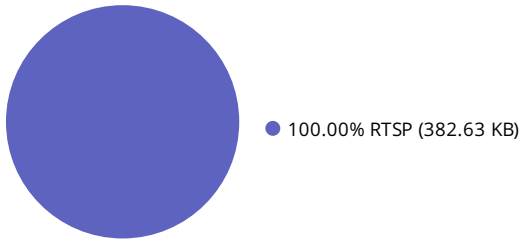
Proxy-Anwendungen

No matching log data for this report

Top-Social-Media-Anwendungen



Top-Video-/Audio-Streaming-Anwendungen



Top-Spieleanwendungen

No matching log data for this report

Top-Peer-to-Peer-Anwendungen

No matching log data for this report

Webnutzung

Das Surfverhalten weist eventuell nicht nur auf eine ineffiziente Verwendung von Unternehmensressourcen hin, sondern ist ggf. auch ein Zeichen für eine suboptimale Webfilter-Richtlinie. Außerdem kann es Einblicke in das allgemeine Surfverhalten der Mitarbeiter gewähren und bei der Festlegung von unternehmensinternen Compliance-Richtlinien helfen.

Top-Webkategorien

#	URL-Kategorie	Benutzer	Anzahl	Bandbreite
1	Information Technology	1	495	7.33 MB
2	Unrated	1	187	373.24 KB
3	News and Media	1	54	11.35 MB
4	Content Servers	1	31	616.86 KB
5	Advertising	1	23	374.01 KB
6	Business	1	16	962.01 KB
7	Search Engines and Portals	1	15	226.51 KB
8	Reference	1	13	438.24 KB
9	Web Hosting	1	12	617.84 KB
10	Meaningless Content	1	11	49.60 KB

In den heutigen Netzwerkumgebungen kommunizieren viele Anwendungen über HTTP – darunter auch einige, von denen man dies eigentlich nicht erwarten würde. Der Hauptvorteil von HTTP besteht darin, dass dieser Kommunikationskanal überall verbreitet, akzeptiert und in den meisten Firewalls (in der Regel) geöffnet ist. Bei den meisten geschäftlichen Anwendungen, die einer Whitelist hinzugefügt wurden, fördert dies im Allgemeinen die Kommunikation. Einige nichtgeschäftliche Anwendungen nutzen HTTP jedoch in unproduktiver oder möglicherweise schädigender Art.

Top-Webanwendungen

#	Anwendungen	Sitzungen	Bandbreite
1	SSL	376	115.39 MB
2	HTTP.BROWSER	632	21.73 MB
3	HTTPS.BROWSER	603	21.39 MB
4	Microsoft.Portal	176	17.76 MB
5	Google.Services	44	7.37 MB
6	Twitter	19	1.10 MB
7	Microsoft.OneNote	21	794.40 KB
8	Dropbox	34	735.62 KB
9	Google.Ads	14	670.44 KB
10	Microsoft.Office.Online	59	565.98 KB

Besuchte Websites

Besuchte Webseiten geben eindeutige Hinweise auf die Nutzung von Unternehmensressourcen durch Mitarbeiter und darauf, wie Anwendungen mit bestimmten Webseiten kommunizieren. Die Analyse der besuchten Domänen kann zu Änderungen in der Unternehmensinfrastruktur führen. Möglich sind unter anderem Webseitensperren, die umfassende Untersuchung Cloud-basierter Anwendungen und die Implementierung von Beschleunigungstechnologien für den Webdatenverkehr.

Meist besuchte Webdomänen

#	Domäne	Kategorie	Besuche
1	www.heise.de	Information Technology	347
2	1.f.ix.de	News and Media	347
3	192.168.0.108	Unrated	187
4	ping.chartbeat.net	Information Technology	176
5	www.fortiguard.com	Information Technology	83
6	jwpltx.com	Information Technology	72
7	www.storage-insider.de	Information Technology	60
8	pagead2.googlesyndication.com	Advertising	35
9	prophet.heise.de	Information Technology	35
10	www.google-analytics.com	Information Technology	31

Schätzungen der Surfzeiten auf individuellen Websites können nützlich sein, um sich einen Einblick in beliebte Websites zu verschaffen. Die Ergebnisse beziehen sich in der Regel auf interne Webressourcen wie Intranets, können jedoch mitunter auch auf eine übermäßige Nutzung hindeuten. Lange Surfzeiten können die Implementierung von Web-Caching-Technologien rechtfertigen oder Anlass zum Erstellen von unternehmensinternen Nutzungsrichtlinien geben.

Top-Websites nach Surfzeit

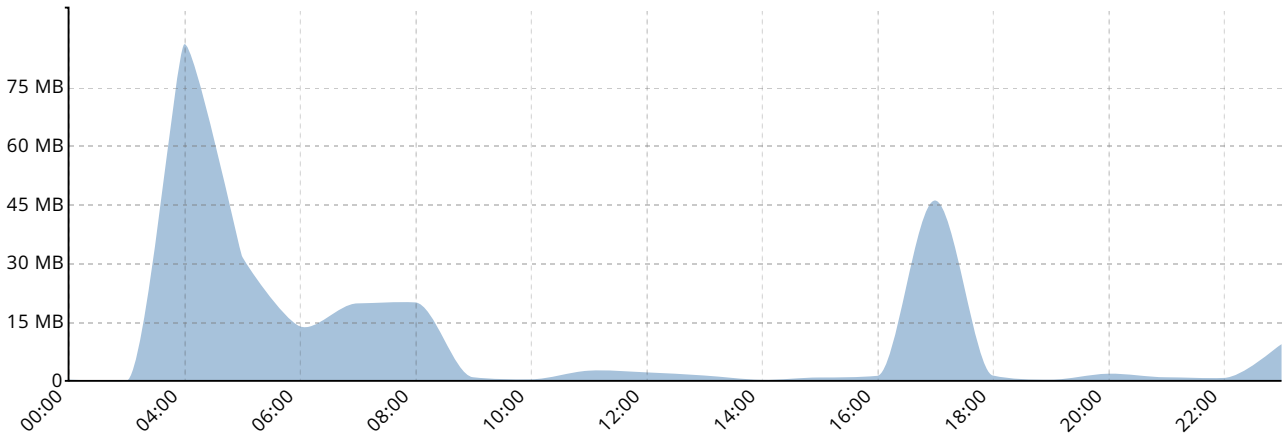
#	Websites	Kategorie	Surfzeit (hh:mm:ss)
1	ping.chartbeat.net	Information Technology	00:37:52
2	www.fortiguard.com	Information Technology	00:03:40
3	gsp1.apple.com	Information Technology	00:02:21
4	wl.dlservice.microsoft.com	Information Technology	00:02:14
5	init-p01st.push.apple.com	Information Technology	00:01:51
6	init-s01st.push.apple.com	Information Technology	00:01:19
7	aia.entrust.net	Information Technology	00:01:19
8	jwpltx.com	Information Technology	00:01:16
9	www.heise.de	Information Technology	00:00:57
10	prophet.heise.de	Information Technology	00:00:50

Netzwerknutzung

Bandbreite

Durch die Analyse der Bandbreitennutzung an einem durchschnittlichen Tag erhalten Administratoren einen verbesserten Einblick in die betrieblichen Anforderungen bezüglich ISP-Verbindungen und Schnittstellengeschwindigkeit. Die Bandbreitennutzung kann auch mittels Drosselung für bestimmte Anwendungen optimiert und während Spitzenverkehrszeiten für bestimmte Benutzer priorisiert werden. Updates lassen sich außerhalb der Arbeitszeiten planen.

Durchschnittliche Bandbreitennutzung pro Stunde



Zu den aussagekräftigsten Bandbreitenanalysen zählt die Prüfung der Ziele und Quellen, die den meisten Datenverkehr generieren. Gängige Ziel-Websites (z. B. externe Websites), etwa für Betriebssystem-/Firmware-Updates, können zur Priorisierung von unternehmenskritischem Datenverkehr gedrosselt werden. Interne Hosts mit hohem Datenverkehrsaufkommen lassen sich durch die Kategorisierung des Datenverkehrs (Traffic Shaping) oder unternehmensinterne Nutzungsrichtlinien optimieren.

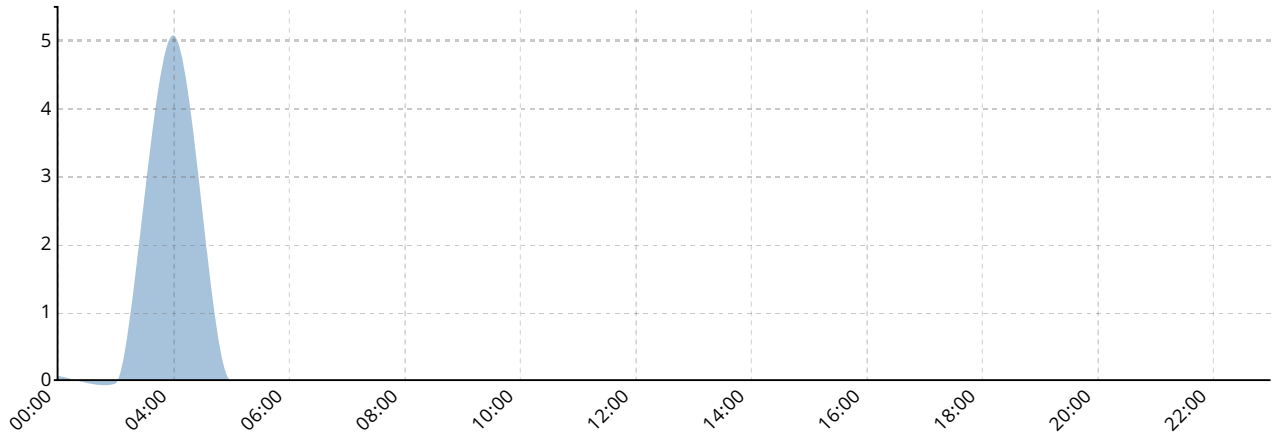
Bandbreitenerschöpfende Top-Quellen/-Ziele

#	Hostname	Bandbreite
1	1.f.ix.de	11.35 MB
2	www.heise.de	3.52 MB
3	media.netapp.com	1.47 MB
4	www.storage-insider.de	731.27 KB
5	files.vogel.de	676.44 KB
6	cormachogan.com	603.58 KB
7	dict.leo.org	406.17 KB
8	cdn.optimizely.com	340.47 KB
9	ping.chartbeat.net	307.19 KB
10	images.vogel.de	255.64 KB

Größenanpassung

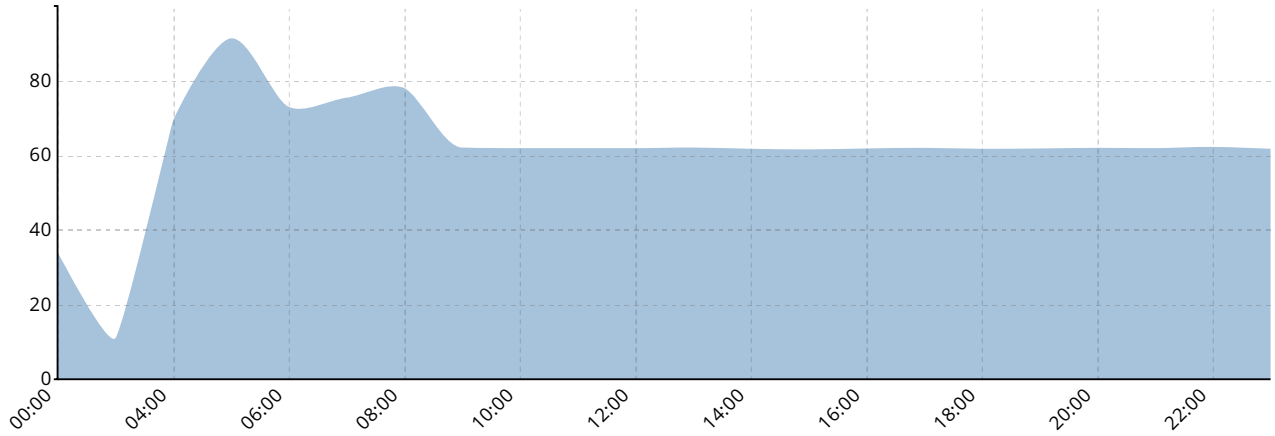
Bei der leistungsbedingten Größenanpassung einer Sicherheitsumgebung ist es von enormem Vorteil, die durchschnittlichen Protokollraten zu kennen. Erhöhte durchschnittliche Protokollraten zu bestimmten Uhrzeiten weisen in der Regel auf Spitzenzeiten bezüglich der Bandbreitennutzung und des Datendurchsatzes hin. Die unternehmensweiten Protokollraten zu berechnen, kann auch bei der Größenanpassung von Upstream-Protokollierungs- und -Analyseanwendungen wie FortiAnalyzer nützlich sein. Beachten Sie, dass bei den hier angegebenen Protokollraten die vollständigen Protokollierungsfunktionen von FortiGate aktiviert waren und diese daher alle Protokolltypen enthalten (Datenverkehr, Antivirus, Anwendung, IPS, Web- und Systemereignisse).

Durchschnittliche Protokollrate pro Stunde



Auch die durchschnittliche Anzahl der innerhalb einer Stunde aufgerufenen Sitzungen kann Hinweise zu Leistungsanforderungen geben (nicht nur für FortiAnalyzer, sondern auch für die letztendlich eingeführte FortiGate-Lösung). Generell besteht zwischen dem Durchsatz, den Protokollraten und der Sitzungslast ein Zusammenhang. Sitzungen sind ein weiterer Datenpunkt, anhand dessen nicht nur die Größe des aktuellen Netzwerks bestimmt, sondern das Netzwerk auch für zukünftige steigende Übertragungsgeschwindigkeiten ausgelegt werden kann.

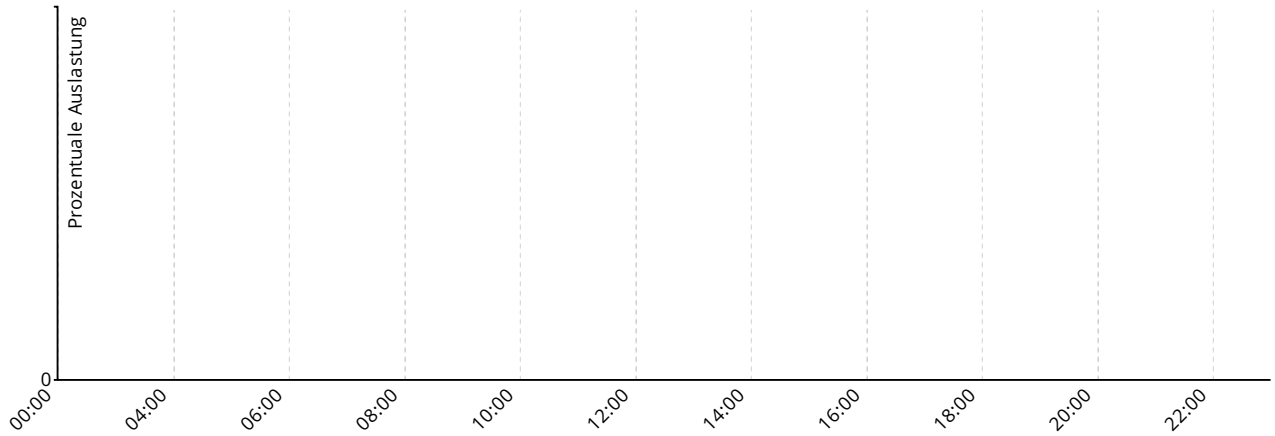
Durchschnittliche stündliche Sitzungslast



Firewall-Statistiken

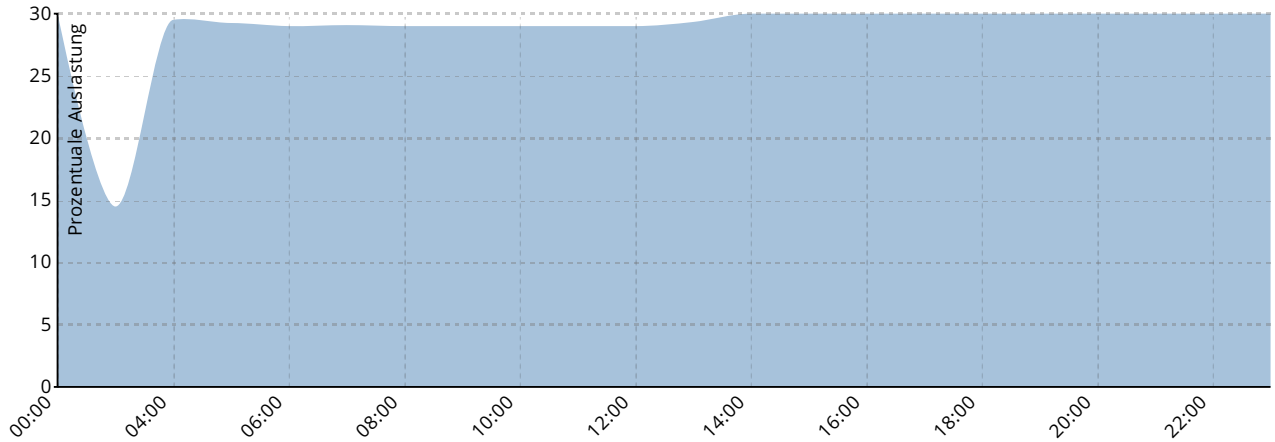
Die Skalierung einer finalen Lösung erfolgt oft anhand der CPU-Auslastung einer FortiGate. Durch die Analyse der stündlich aufgeschlüsselten CPU-Auslastung lässt sich die Leistung von FortiGate-Plattformen im Zielnetzwerk leicht abschätzen. Bei einem höheren Durchsatz werden meist auch mehr Protokolle generiert. Wird eine Auslastung von 75 % oder mehr über einen längeren Zeitraum verzeichnet, sind für die endgültige Implementierung möglicherweise ein neues Modell oder eine überarbeitete Architektur erforderlich.

Durchschnittliche stündliche CPU-Auslastung durch FortiGate



Gleichermaßen bietet die Ermittlung der Speicherauslastung innerhalb eines bestimmten Zeitraum einen Hinweis auf die Nachhaltigkeit eines FortiGate in der Zielnetzwerkumgebung. Die Speicherauslastung kann aufgrund von aktuellen oder ausstehenden Protokollierungsaktivitäten auch bei geringem Durchsatz hoch bleiben.

Durchschnittliche stündliche Speicherauslastung durch FortiGate



FortiGuard-Sicherheit und -Services

Um eine effektive Sicherheit zu gewährleisten, ist es wichtig, die Bedrohungslandschaft zu kennen und schnell auf mehreren Ebenen reagieren zu können. Die Cyber-Landschaft wird täglich von Hunderten Forschern bei FortiGuard Labs durchkämmt, um aufkommende Bedrohungen zu entdecken und effektive Gegenmaßnahmen zum Schutz von Unternehmen auf der ganzen Welt zu entwickeln. Dank ihres Engagements konnte FortiGuard bereits über 250 Zero-Day-Bedrohungen und Schwachstellen entdecken. Dies ist auch der Grund, warum Sicherheitslösungen von Fortinet bei Tests von NSS Labs, Virus Bulletin, AV Comparatives und anderen Anbietern hinsichtlich der realen Sicherheitseffektivität so gut abschneiden.

Applikationskontrolle und IPS der nächsten Generation

Die Applikationskontrolle und Intrusion Prevention (IPS) zählen zu den grundlegenden Sicherheitstechnologien von Firewalls der nächsten Generation wie FortiGate. Organisationen auf der ganzen Welt vertrauen bei der Anwendungsverwaltung und der Abwehr von Netzwerkangriffen auf die FortiGuard-Applikationskontrolle und die IPS-Funktion der FortiGate-Plattform (FortiGuard blockiert täglich rund 470.000 Angriffsversuche.) Die Effektivität der auf FortiGate-Plattformen ausgeführten Applikationskontrolle und IPS wird von NSS Labs in Branchenvergleichen getestet und durchgängig als „Empfohlen“ bewertet.

Web Filtering

FortiGuard Labs verarbeitet rund um die Uhr ca. 43 Millionen URL-Kategorisierunganforderungen und blockiert 160.000 infizierte Websites. Der Web Filtering-Service bewertet über 250 Millionen Websites und liefert wöchentlich knapp 1,5 Millionen neue URL-Bewertungen. FortiGuard ist die einzige von VBWeb zertifizierte Webfilterlösung. In den 2016 durchgeführten Tests erreichte sie eine Blockierung von 97,7 % direkter Malware.

Virenschutz und mobile Sicherheit

FortiGuard Labs neutralisiert rund um die Uhr ca. 95.000 Malware-Programme, die konventionelle, mobile und IoT-Plattformen bedrohen. Dank patentierter Technologien kann der Antivirus-Service von FortiGuard Tausende aktuelle und zukünftige Malware-Varianten mit einer einzigen Signatur identifizieren. Dies optimiert sowohl die Sicherheitseffektivität als auch die Leistung. Fortinet erhält bei Branchentests von Virus Bulletin und AV Comparatives konsistent erstklassige Bewertungen hinsichtlich der Effektivität.

Spamschutz

FortiGuard Labs blockiert rund um die Uhr ca. 21.000 Spam-E-Mails. Darüber hinaus liefert es jede Woche ca. 46 Millionen neue und aktualisierte Spam-Regeln. E-Mails sind der primäre Vektor für den Start fortschrittlicher Angriffe auf eine Organisation. Eine Sicherheitsstrategie bedarf daher unbedingt einer hocheffektiven Antispam-Lösung.

Schutz vor komplexen Bedrohungen (FortiSandbox)

Tausende von Organisationen auf der ganzen Welt nutzen FortiSandbox zur Identifizierung komplexer Bedrohungen. FortiSandbox wird bei Branchentests von NSS Labs unter den Breach Detection Systems (BDS) konsistent als „Empfohlen“ bewertet. IN den NSS Labs-Tests 2015 erreichte die Lösung zudem eine Aufdeckungsrate von über 97 %.

IP-Reputationsservice

FortiGuard Labs blockiert rund um die Uhr ca. 32 000 Botnet Command & Control (C&C)-Kommunikationsversuche. Ein wichtiger Teil der Bedrohungskette ist die Kommunikation der Bedrohung mit einem Command & Control-Server einer Organisation – entweder, um weitere Bedrohungen herunterzuladen oder gestohlene Daten zu extrahieren. Diese Kommunikation wird infolge der Bewertung der Zuverlässigkeit von IP- und Domänenadressen blockiert, um Bedrohungen zu neutralisieren.