F

Firewalls

Buyer's Guide and Reviews

October 2018

Get a custom version of this report...personalized for you!

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station community. We offer a [customized report](#) personalized for you based on:

- Your industry
- Company size
- Which solutions you're already considering

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

[Get your personalized report here.](#)

Contents

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Vendor Directory

A10 Networks	A10 Networks Thunder CFW		**Juniper**	Juniper SRX
Barracuda Networks	Barracuda NextGen Firewall		**McAfee**	McAfee StoneGate
Check Point	Check Point Power-1		**McAfee**	McAfee Firewall Enterprise MFE
Check Point	Check Point UTM-1		**NetFortris**	NetFortris Hosted Firewall
Check Point	Check Point VPN-1		**NetFortris**	NetFortris Threat Analyzer
Check Point	Check Point VSX		**OPNsense**	OPNsense
Check Point	Check Point Next Generation Firewall		**Palo Alto Networks**	Palo Alto Networks VM-Series
Cisco	Cisco Sourcefire Firewalls		**Palo Alto Networks**	Palo Alto Networks Next-Generation Firewall
Cisco	Cisco ASA		**pfSense**	pfSense
Cisco	Meraki MX Firewalls		**Sangfor**	Sangfor NGAF
Cisco	Cisco Firepower NGFW		**Sonatype**	Sonatype Nexus Firewall
Cisco	Cisco ASAv		**SonicWall**	SonicWall TZ
Cisco	Cisco IOS Security		**SonicWall**	SonicWall NSA
Comodo	Comodo Dome Firewall		**Sophos**	Sophos Cyberoam UTM
Fortinet	Fortinet FortiGate		**Sophos**	Sophos UTM
Fortinet	FortiGate-VM		**Sophos**	Sophos XG
Fortinet	Fortinet FortiOS		**Stormshield**	Stormshield Network Security
GFI	Kerio Control		**Trustwave**	Trustwave Firewalls
Hewlett Packard Enterprise	3Com H3C Firewall		**Untangle**	Untangle NG Firewall
Hillstone Networks	Hillstone E-Series		**WatchGuard**	WatchGuard XTM
Hillstone Networks	Hillstone T-Series		**WatchGuard**	WatchGuard Firebox
Hillstone Networks	Hillstone X-Series Data Center Firewalls		**Zscaler**	Zscaler Web Security
Hillstone Networks	Hillstone CloudEdge			

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Top Firewalls Solutions

Over 293,441 professionals have used IT Central Station research. Here are the top Firewalls vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key

● **Views**
Number of views

● **Comparisons**
Number of times compared to another product

● **Reviews**
Total number of reviews on IT Central Station

● **Followers**
Number of followers on IT Central Station

● **Average Rating**
Average rating based on reviews

Bar length

The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows: The product with the highest count in each area gets the highest available score. (20 points for **Reviews**; 16 points for **Views**, **Comparisons**, and **Followers**.) Every other product gets assigned points based on its total in proportion to the #1 product in that area. For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's score for reviews would be 20% (weighting factor) * 80% = 16. For **Average Rating**, the maximum score is 32 points awarded linearly based on our rating scale of 1-10. If a product has fewer than ten reviews, the point contribution for Average Rating is reduced (one-third reduction in points for products with 5-9 reviews; two-thirds reduction for products with fewer than five reviews). Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

1   Fortinet FortiGate

194,276 views   **107,768** comparisons   **33** reviews   **4,660** followers   **8.4** average rating

2   Cisco ASA

95,908 views   **54,965** comparisons   **66** reviews   **4,433** followers   **7.8** average rating

3   Sophos UTM

93,665 views   **54,148** comparisons   **17** reviews   **3,051** followers   **8.8** average rating

4   pfSense

76,372 views   **47,710** comparisons   **21** reviews   **2,892** followers   **8.7** average rating

5   Meraki MX Firewalls

37,361 views   **23,154** comparisons   **10** reviews   **676** followers   **9.3** average rating

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

6 Sophos Cyberoam UTM

29,152 views   **16,590** comparisons   **14** reviews   **1,194** followers   **8.4** average rating

7 WatchGuard XTM

35,066 views   **22,927** comparisons   **10** reviews   **643** followers   **7.9** average rating

8 Juniper SRX

29,331 views   **19,721** comparisons   **14** reviews   **637** followers   **7.8** average rating

9 SonicWall TZ

38,011 views   **25,348** comparisons   **7** reviews   **1,456** followers   **8.6** average rating

10 SonicWall NSA

15,347 views   **12,017** comparisons   **11** reviews   **529** followers   **7.3** average rating

Top Solutions by Ranking Factor

🔴 Views

SOLUTION	VIEWS
1	Fortinet FortiGate	194,276
2	Cisco ASA	95,908
3	Sophos UTM	93,665
4	pfSense	76,372
5	SonicWall TZ	38,011

🟢 Reviews

SOLUTION	REVIEWS
1	Cisco ASA	66
2	Fortinet FortiGate	33
3	pfSense	21
4	Sophos UTM	17
5	Juniper SRX	14

🔵 Followers

SOLUTION	FOLLOWERS
1	Fortinet FortiGate	4,660
2	Cisco ASA	4,433
3	Sophos UTM	3,051
4	pfSense	2,892
5	SonicWall TZ	1,456

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Fortinet FortiGate　　See 33 reviews >>

Overview

The FortiGate family of NG firewalls provides proven protection with unmatched performance across the network, from internal segments, to data centers, to cloud environments. FortiGates are available in a large range of sizes and form factors and are key components of the Fortinet Security Fabric, which enables immediate, intelligent defense against known and new threats throughout the entire network.

SAMPLE CUSTOMERS

Pittsburgh Steelers, LUSH Cosmetics, NASDAQ, Verizon, Arizona State University, Levi Strauss & Co.
Whitepaper and case studies here

TOP COMPARISONS

Cisco ASA vs. Fortinet FortiGate ... Compared 18% of the time [See comparison]
Sophos UTM vs. Fortinet FortiGate ... Compared 15% of the time [See comparison]
Palo Alto Networks WildFire vs. Fortinet FortiGate ... Compared 13% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 15%
Comms Service Provider ... 10%
Government ... 7%
Manufacturing Company ... 6%

COMPANY SIZE

1-200 Employees ... 33%
201-1000 Employees ... 38%
1001+ Employees ... 28%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Comms Service Provider ... 12%
Real Estate/Law Firm ... 12%
Energy/Utilities Company ... 12%
Construction Company ... 8%

COMPANY SIZE

1-200 Employees ... 48%
201-1000 Employees ... 30%
1001+ Employees ... 21%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Fortinet FortiGate

Top Reviews by Topic

VALUABLE FEATURES

Andrew S. Baker (ASB)

* The CLI is robust and powerful, enabling rapid, consistent changes via SSH. The device identification is very flexible, facilitating the creation of rules to regulate all sorts of devices that might spring up on a network, especially via WiFi. * The IPsec tunnels are very easily created, and quite interoperable with devices from other vendors. * WAN load-balancing has improved, but needs some refinement. You can set up a different DDNS config for each WAN link. It is great to be able largely use the same OS features across the family of devices. [Full Review]

Cesar Nieves

It's a complete solution. You can purchase switches and you don't need to do anything with them. You just put in the firewall and the switches get all the policies and rules that you already have in the firewall. That's a very nice feature because with, for example, Cisco, you need to set the switch, you need to set the firewall, and you need to test it. With Fortinet, you just connect the FortiSwitch to the Fortinet and that's it. It's very easy. In the last version of the FortiOS - the operating system of the firewall - they put a lot of new featu... [Full Review]

Diana Nongera

* DHCP functionality: The object tab where we manage our IP addresses and static. The DHCP monitors them. * FortiClient: You can easily connect when you are home, check out what you want to do, and connect to your network when you are not at work. You can switch on servers and you can check what is wrong. [Full Review]

reviewer32902

* The prompt and knowledgeable support behind them. * Their reliability and their policy of pre-shipping replacements when a unit has failed. * The simplicity and clarity of their user interface and documentation. * Their 'cookbooks' that walk you through the most common installation scenarios. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

Andrew S. Baker (ASB)

The first implementation I performed of a FortiGate 200D was to replace a Juniper SSG-140 in a main corporate office. This implementation provided improved network administration and network performance. We also received more timely security updates, and it became easier to connect all of the other offices together (via an IPsec VPN mesh). As additional FortiOS releases have come out, we have obtained more flexibility in device identification and WAN load-balancing, among other things. [Full Review]

Cesar Nieves

The first benefit is the cost. It is very affordable. Also, it's very easy to set up, it's very easy to make policies and, for an organization, that means you don't need IT expert in firewalls. You just need to have somebody who knows a little bit of IT, and that's it. With other products, you need someone with a "Masters" degree in firewalls. [Full Review]

MnG32

We have peace of mind. We do work in a very dangerous environment, the internet, and this device gives us alerts. It gives us the opportunity to know what is going on. [Full Review]

Fortinet FortiGate

ROOM FOR IMPROVEMENT

Andrew S. Baker (ASB)

WAN load-balancing could be a lot better at detecting when a link is poor or inconsistent, and not just flat out dead. There are lots of options for routing traffic over a specific path when you have WAN load-balancing enabled, but they are not as clear and consistent as they could be, and most can only be set at the CLI. Some configuration elements cannot be easily altered once created. For instance, there is no way to rename an interface (say, for a VPN tunnel), unless you create an entirely new one and perform a little gymnastics to switch from o... [Full Review]

Chingiz Abdukarimo v

I think there could be more QoS features in GUI. FortiGate and manual queue assignment. Also a few ports supporting native vlan while in trunk mode would be very helpful in some cases. [Full Review]

MnG32

I would like to be able to do segmentation, for a specific user, with more priveledges. I would also like to see an easier user interface to implement that. [Full Review]

Simon Chaba

1. sFlow and NetFlow I could not configure sFlow from the FortiGate graphical user interface. I realized that the sFlow configuration is available only from the CLI, and discovered that sFlow is not supported on virtual interfaces, such as VDOM links, IPsec, or GRE. NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic. It is not supported on FortiGate for those who have a NetFlow analyzer/collector already setup in their network. 2. Policies To control traffic in a firewall, you need t... [Full Review]

PRICING, SETUP COST AND LICENSING

Andrew S. Baker (ASB)

Licensing and setup costs are generally pretty clear with Fortinet. If you go with centralized management or their Log Analyzer tool, these carry some additional pricing that you need to look at. Check out the price matrix, and go with a value-added reseller that understands how to help you size out the equipment. Remember to always look at the performance with the assumption that you will have many of the unified threat management (UTM) features on, not off. [Full Review]

Cesar Nieves

Pricing is good. They offer a lot of things, the most important is the support. Every time you upgrade your license, you also get insurance for the equipment. If you have any problem with equipment, they send in new equipment. [Full Review]

reviewer329 02

Pricing and licensing have to be taken in context with value. Fortinet is usually not the least expensive alternative when considering an upfront investment, but if you take into account the support costs over several years, they are often as cost-effective as the 'cheaper' solutions. [Full Review]

Cisco ASA

Overview

Adaptive Security Appliance (ASA) is Cisco's end-to-end software solution and core operating system that powers the Cisco ASA product series. This software solution provides enterprise-level firewall capabilities for all types of ASA products, including blades, standalone appliances and virtual devices. Adaptive Security Appliance provides protection to organizations of all sizes, and allows end-users to access information securely anywhere, at any time, and through any device.Adaptive Security Appliance is also fully compatible with other key security technologies, and so provides organizations with an all-encompassing security solution.

SAMPLE CUSTOMERS

There are more than one million Adaptive Security Appliances deployed globally. Top customers include First American Financial Corp., Genzyme, Frankfurt Airport, Hansgrohe SE, and City of Tomorrow.

TOP COMPARISONS

Fortinet FortiGate vs. Cisco ASA ... Compared 33% of the time [See comparison]
Palo Alto Networks WildFire vs. Cisco ASA ... Compared 12% of the time [See comparison]
Juniper SRX vs. Cisco ASA ... Compared 8% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 17%
Comms Service Provider ... 11%
Manufacturing Company ... 8%
Government ... 7%

COMPANY SIZE

1-200 Employees ... 30%
201-1000 Employees ... 29%
1001+ Employees ... 40%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 18%
Comms Service Provider ... 13%
Manufacturing Company ... 10%
Retailer ... 8%

COMPANY SIZE

1-200 Employees ... 36%
201-1000 Employees ... 30%
1001+ Employees ... 34%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Cisco ASA

Top Reviews by Topic

💡 VALUABLE FEATURES

Jijish Gopi

If you compare it with other products, other firewall products in the market, at this moment, it doesn't have that many features, no impressive feature in it, in fact. The one thing I like about the product is the logging features, the way it logs, the way it forwards the logs in Syslog. It generates the particular Syslog. Compared to other products, that is the only feature, I feel, that is good. I have worked with other firewall products, so I know it very well. The logs are pretty good. Then it forwards. When it forwards the logs to a third-party... [Full Review]

Neil McFadyen

* Most of same old ASA 5520 config could be used for the new 5516-X model. The ASDM interface is improved and can also be configured to the Firepower settings. * I am used to the ASA syntax, therefore it is quite easy to make up new rules. I have found that DNS doctoring rules are useful, and I am not sure how other firewalls handle the issue of internal versus external DNS, so this was a reason to keep the same type of firewall. * Customizing logging event of syslog to feed into Splunk is very useful for management and monitoring just for the impor... [Full Review]

ipmplspr538 920

All features provided by the platform are quite the same for all other platforms. We rather missed some features we were used to, such as virtual routers [Full Review]

Christina Phillips, MBA

I find the overall capability of the higher end firewall products to handle most network tasks without any issues. In addition, it is easy to train lower level help desk personnel on the GUI management. [Full Review]

📄 IMPROVEMENTS TO MY ORGANIZATION

Frank Theilen

The ASA 55-x range is a solid and reliable firewall. It secures the traffic for normal purposes. If you ask how a firewall can improve our business: It can't. It is securing our business IT network. But if you want to know what the ASA5520 can do to secure our network: Not much more than any firewall. It is a solid port firewall, nothing more, nothing less. [Full Review]

In432TchMn 89

The ASAs are very stable firewalls, and they've been very good at protecting our assets here at the bank. They have done exactly what they were purchased for. They have done a great job. [Full Review]

Neil McFadyen

It works better through specs than our old ASA 5520. It seems to perform the same functionality unless you buy the additional threat protection licenses, so this is a disappointment. I found a bug where the ASDM could not be used with Windows 2016, but it did work with Windows 10. [Full Review]

Cisco ASA

ROOM FOR IMPROVEMENT

Jijish Gopi

It doesn't have a proper GUI to do troubleshooting, so most people have to rely on the command line. Its a sort of legacy product nowadays. The firewalls which are the next generation have loads of features added to them, and they are all in one box. It should have packets, deep level inspections and controls, like the features which other IPS solutions have. It just doesn't have any. It's just a box which does firewalling. Threat management features also should be added into it. So, the first thing is that the GUI has to be improved. The second thi... [Full Review]

Frank Theilen

Firewalls, in general, were not really designed for normal IT personnel, but for firewall and network experts. Therefore, they missed a lot of options and did not provide any good reporting or improvement options. For example, to update or add a feature, you end up buying new support and licenses. The process is complex and changes so rapidly that you won't find a salesperson who will offer you the right products. New generation firewalls are cloud managed or provide a good interface. They integrate into the environment. They are application aware a... [Full Review]

In432TchMn 89

The only con that I have really seen with it is the reporting structure. FirePOWER is good. It has been a great help because, before that, it was not good at all. [Full Review]

Neil McFadyen

* It is confusing to have two management interfaces, e.g., ASDM and Firepower Management Center. It would be nice to have a Windows program instead of a virtual appliance for the Firepower Management Center. The ASA and Firepower module seem redundant, not sure which one to set the rules in, but maybe that was for backward compatibility. I am not sure that is very useful. * It is surprising that you need to have a virtual appliance for the Firepower Management Center. It is not good if you have to setup a VMware server just for it. * 10Gb interfaces... [Full Review]

PRICING, SETUP COST AND LICENSING

Frank Theilen

If you look for user internet access, many new products can help with filtering and rules or procedures, like Meraki. This replaces the purpose of proxy servers. If you have to secure web servers from the internet, you need a decent firewall with web features to process the requests and redirect traffic to web servers. Cisco is no longer the only vendor offering these features. With Microsoft TMG out of the race, others have to push in. But firewalls are also no longer the first frontier of security. Cloud services are in there as well. [Full Review]

In432TchMn 89

The cost of keeping the licensing up on the ASA is very expensive. It has a lot of positives, but the cost of going with it is really starting to be a major negative right now. [Full Review]

Neil McFadyen

ASA pricing seems high compared to other firewalls, such as the Sophos XG models. The licensing features are getting more complicated. These should be simplified. [Full Review]

![S] **Sophos UTM**   [See 18 reviews >>](#)

Overview

The global network of highly skilled researchers and analysts, protecting businesses from known and emerging malware - viruses, rootkits and spyware.

SAMPLE CUSTOMERS

One Housing Group

TOP COMPARISONS

Fortinet FortiGate vs. Sophos UTM ... Compared 31% of the time [See comparison]
pfSense vs. Sophos UTM ... Compared 25% of the time [See comparison]
WatchGuard XTM vs. Sophos UTM ... Compared 6% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 8%
Comms Service Provider ... 8%
Retailer ... 8%
Non Tech Company ... 7%

COMPANY SIZE

1-200 Employees ... 46%
201-1000 Employees ... 36%
1001+ Employees ... 18%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Mining And Metals Company ... 14%
Legal Firm ... 14%
Government ... 14%
Construction Company ... 14%

COMPANY SIZE

1-200 Employees ... 67%
201-1000 Employees ... 11%
1001+ Employees ... 22%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Sophos UTM

Top Reviews by Topic

💡 VALUABLE FEATURES

See more Valuable Features >>

Joseph Mallozzi

The most valuable to features are: Web Application Firewall, Sophos UTM Manager, IDS/IPS, Remote Access, and RED. * WAF: This is excellent for hardening web servers. The firewall will reverse proxy your web servers, eliminating the need to open ports. Instead the firewall will run an instance of Apache and proxy all traffic to and from the real web servers. (This is also handy when you have a single public IP.) * SUM: The Sophos UTM Manager is a must have for any MSP. The SUM is a centralized portal for quick access to all the firewalls you manage. ... [Full Review]

EtienneLieb etrau

The UTM/SG platform starts off with the basic functionality of being a good Firewall, adding the additional modules opens up the products set and allows for full web filtering and application control, reverse proxy, APT detection, IPS, VPNs, User portal etc. The licensing model works very nicely to allow you to get the right protection at the right price point for the right deployment size. In the increasingly cloud focused word the Sophos UTM's ability to deliver Safe web access, Web Filter and Cloud Application control has gone from being a nice t... [Full Review]

M.K. Goyal

* A good package overall * A nice UTM appliance with a good GUI and reports. * Configuring web access controls in the appliance is a bit typical and requires debarring and listing separately. Once configured, the solution works beautifully. [Full Review]

Dragan Pavlovski

All the features are valuable. * Web protection: Allows me to control unnecessary web traffic into the company network. * Email protection: Protects the company from spam and malicious emails. * RED and VPN: Provides an easy and secure way to connect branch offices so I can easily control them. * WAF and DMZ: Provides an easy and very secure way to publish your internal servers. Enables you to have more than one WAN and to use them for load balancing and controlling the traffic through them. [Full Review]

📄 IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Joseph Mallozzi

The UTM product has definitely improved the way our organization functions. We have set a standard across clients and engineers. Everyone is trained on the product and knows how to manage the devices. UTM is probably the most complete all-in-one firewall that I have used to date. Having the UTM Manager has probably made the most impact, with over 150 firewalls in our portal, management and monitoring have never been easier. [Full Review]

Ayodele Mumuni

* It has allowed us to have one solution for our AWS needs. * It allows our developers to be able to securely log into servers to deploy and manage software. * It has allowed us to design a bespoke cloud space for our clients, while still having an excellent level of protection. [Full Review]

EtienneLieb etrau

The Sophos UTM planform has allowed us to improve or implement the following security practices: * Details Web filtering and user access Control * SaaS QoS * Network segmentation with firewall and IPS * WiFi protection * Web Application Proxy everywhere, inside and out * WAN expansion with SSL VPN and IPsec VPN over the Internet * Two Factor Authentication requirement for PCI compliance * Reduced the need for expensive MPLS deployments [Full Review]

Sophos UTM

📊 ROOM FOR IMPROVEMENT

Ayodele Mumuni

You per availability, zone, and per VPC. It should offer an account-based solution. When you buy a Sophos license, you have to buy a license for each location. We have clients in the US. We have clients in Ireland. We have clients in the UK. With GD-PI coming, the clients' data needs to stay in-house, so when you buy the Sophos license, it only works for the UK. Then, you have to buy another in the USA and another one in Ireland, then you have to have a VPN tunnel between all of them to have them talk to each other because Sophos blocks them talking... [Full Review]

EtienneLieb etrau

At Enterprise level the SUM (UTM Manager) needs to be updated to reflect all of the capabilities At the Reporting level for user internet browsing the On-box Reporting is very basic and even adding the Sophos iView only give you limited improvement. Having said that, Fastvue's Sophos Reporter provides all of this and more and integrates seamlessly with the UTM platform to unlock all of the log data's value. The SG platform does however not scale to a large enterprise deployment. You can deploy at scale but this is where the platform shows its age an... [Full Review]

Jeff Berndsen

I wish the internet failover worked better. As it stands right now, when we have an internet failure on WAN1, it takes several minutes before our WAN2 connection picks up the traffic, with many things not working until I manually fail over to the other WAN. [Full Review]

M.K. Goyal

Initially, there were problems of wireless access points not getting detected and lease lines were getting disconnected after one hour. Sophos replaced the appliance, but the issue was not resolved . The matter got escalated to their international support and the issue was identified as a bug where long distance fiber connections are used over single mode fiber. The patch was shipped by Sophos with a promise to fix the issue in the next release. Now, the appliance is working fine. The issue of wireless access points was due to some compatibility iss... [Full Review]

⚙️ PRICING, SETUP COST AND LICENSING

Joseph Mallozzi

I am not in sales and cannot comment on this. I design and implement network configurations. I would recommend to follow Sophos' sizing guidelines for choosing which license and model to use. Sophos has their own way of going about this and supplies partners with all the information required. If you follow their documentation and guidelines, there should be zero questions about licensing and sizing. Sophos also offers free training when selling their products from within the partner portal. [Full Review]

Ayodele Mumuni

Licensing is a bit complicated, as it is based on products -- so define your requirements and find what best suits you, as you do not need the whole suite of software they provide. For AWS, it is pretty straightforward. You buy it, then you have all your licenses that you need, approximately 60 or 70, or it might even be unlimited. However, that is for one margin to expand to different margins. If you have an on-premise AWS, or one of our clients wanted on-premise AWS licenses, that is for the first module. So if you expand to second module, you hav... [Full Review]

EtienneLieb etrau

The licensing options with virtual are great and scaling up and down is typically not an issue if you reseller is involved. Sometimes buying the hardware makes more sense than going virtual. The hardware is great and unlike the virtual licensing is unrestricted by user numbers. There are huge numbers of OS models that range from very small to very large. You will likely find a good fit for your deployment. A great benefit is that you can migrate your Sophos SG license to a Sophos XG license in the future. You can safely Deploy on SG and later migrat... [Full Review]

pfSense

Overview

Providing comprehensive network security solutions for the enterprise, large business and SOHO, pfSense solutions bring together the most advanced technology available to make protecting your network easier than ever before. Our products are built on the most reliable platforms and are engineered to provide the highest levels of performance, stability and confidence.

SAMPLE CUSTOMERS

Nerds On Site Inc., RKC Development Inc., Expertech, Fisher's Technology, Ncisive, Consulting, CPURX, Vaughn's Computer House Calls, Imeretech LLC, Digital Crisis, Carolina Digital Phone, Technigogo Technology Services, The Simple Solution, SwiftecITInc, Rocky Mountain Tech Team, Free Range Geeks, Alaska Computer Geeks, Lark Information Technology, Renaissance Systems Inc., Cutting Edge Computers, Caretech LLC, GoVanguard, Network Touch Ltd, P.C. Solutions.Net, Vision Voice and Data Systems LLC, Montgomery Technologies, Techforce, Concero Networks, ASONInc, CPS Electronics and Consulting, Darkwire.net LLC, IT Specialists, MBS-Net Inc., VOICE1 LLC, Advantage Networking Inc., Powerhouse Systems, Doxa Multimedia Inc., Pro Computer Service, Virtual IT Services, A&J Computers Inc., Envision IT LLC, CommunicaONE Inc., Bone Computer Inc., Amax Engineering Corporation, QPG Ltd. Co., IT 101 Inc., Perfect Cloud Solutions, Applied Technology Group Inc., The Digital Sun Group LLC, Firespring

TOP COMPARISONS

Sophos UTM vs. pfSense ... Compared 29% of the time [See comparison]
Fortinet FortiGate vs. pfSense ... Compared 17% of the time [See comparison]
Cisco ASA vs. pfSense ... Compared 9% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Comms Service Provider ... 15%
Manufacturing Company ... 9%
Financial Services Firm ... 8%
Non Tech Company ... 6%

COMPANY SIZE

1-200 Employees ... 40%
201-1000 Employees ... 37%
1001+ Employees ... 23%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Comms Service Provider ... 16%
University ... 16%
Energy/Utilities Company ... 11%
Construction Company ... 11%

COMPANY SIZE

1-200 Employees ... 66%
201-1000 Employees ... 23%
1001+ Employees ... 11%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

pfSense

Top Reviews by Topic

VALUABLE FEATURES

Koen Van Cauwenberghe

* I can manage it easily by myself. * The interaction between the same firewalls is good. We can connect VPNs over the same firewall easily. * It is an open source solution. Therefore, the price is good. * OPNsense. * The performance and functionality are good. [Full Review]

Christopher Collins

* The VPN and the firewall. They are reliable and easy to manage. * The VPN is valuable for setting up secure remote connections to our network. * pfSense has the OpenVPN package which is a well-supported VPN software. * The "OpenVPN Client Export" package is really helpful in exporting the VPN client software on most popular devices: iOS/Android, Windows, Mac, Linux, and a handful of SIP handsets. [Full Review]

COO998b301

The most valuable feature: It is easy to manage. I don't have to have highly trained engineers. A mid-level employee who is conversant with firewalls can take care of managing it. It's the 90 percent/10 percent equation. They can perform 90 percent of the required tasks with 10 percent of the knowledge. The IPsec and VPN services, as well as the interoperability with other solutions such as Cisco, Juniper, and Palo Alto have been invaluable. [Full Review]

Richard McAlexander

I use pfSense because it gives me the flexibility to greatly expand basic firewall features. It's open source (and free - as in beer and speech), but also has commercial support. This can be run on any commodity hardware on the market (I've ran it on AMD and Intel - even Atom, processors) and throughput is excellent, even with lower speed CPUs and less RAM. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

Koen Van Cauwenberghe

I do not have any big malware in my network, partly because of pfSense. The firewall blocks every malfunctioning malware or virus. Also, the access from outside our network has to be blocked, and I know by experience that our pfSense is very closed. You have to open every port in order to make sure that there can be a connection from outside our network. [Full Review]

COO998b301

The web management interface is ridiculously easy to utilize, even for the junior engineers on staff. Given the ease of use, this solution has minimized staff and training costs considerably. The ability to integrate packages, such as OpenRADIUS, Snort, and Squidguard has minimized server sprawl. The capability to run as a VM on a hypervisor, such as ESXi, makes this solution easy to implement and manage. [Full Review]

Richard McAlexander

I stood up pfSense in a Large Telecom providers Lab environment for their next generation products. I was able to achieve 10G throughput (about 9.1 true throughput as tested over 4 days solid), and only hit a max of 20% CPU utilization on a DL380 G7. This server also had Suricata (in IPS mode and a heavy ruleset), as well as pfBlocker running. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

pfSense

ROOM FOR IMPROVEMENT

Koen Van Cauwenberghe

A malware blocker should be included. I do not know if it is included yet. However, until now, we have not experienced a large malware invasion. There are a few features not included, and when you have to use those features, you have to pay for them. I know that I should change the current pfSense solution. I should change it because we have only one key port on it. Our internet access also has a key port now, I should have two key ports, one to the LAN and one to the WAN. Therefore, I want to change it, because it gives us less speed. I could provi... [Full Review]

Christopher Collins

Network monitoring and device inventory could use some improvements. I'm using SpiceWorks for this because it never really worked in pfSense. Network monitoring is a big topic and I realize there is plenty of software out there like SpiceWorks, NTOPNG, PDQ, Zabbix, and Nagios. I can easily log into pfSense and check "Status > Gateways" to see if the internet connection is online. However, I don't usually know if there's a problem until it's been down for a while and someone tells me about it. I realize this is a tricky problem, because if the pfSens... [Full Review]

COO998b301

They need to take care of a few issues with the GUI. Occasionally, they don't update the configurations properly. I would also like them to firm up the VPN aspect of the software a bit and provide better monitoring software. When a carrier that supports a VPN or IPsec tunnel bounces, the recovery time can take a few minutes. Reducing that time would be greatly appreciated in future releases. [Full Review]

Reinhardt Jansen

Layer 7 filtering has been taken away from pfSense. They would like us to use Snort, which is a good thing, but I would like them to make the Layer 7 thing easier. The one reason that we did not go with pfSense is that it is not centrally managed like Meraki, where you log into the website and can see all your services there. This is the only reason why we are going with Meraki. We would like to be able to see is all the configurations from a central interface on all our pfSenses. [Full Review]

PRICING, SETUP COST AND LICENSING

COO998b301

In comparison to a lot of other solutions, it's very inexpensive. It is a great solution that is economical. It scales so the cost per protected MB is almost free. [Full Review]

Gustavo Rendon

If you need to buy hardware onto which to install PfSense, go with their boxes on their website, they are great. If you already have the hardware, just download and install, it works great either way. [Full Review]

Matt Bilbrey

Unless they have specific requirements that demand a particular device, I always suggest pfSense specifically because of the absence of pricing and licensing. [Full Review]

Meraki MX Firewalls

Overview

With the proliferation of modern applications and mixed-use networks, host and port based security is no longer sufficient. Cisco Meraki's layer 7 "next generation" firewall, included in MX security appliances and every wireless AP, gives administrators complete control over the users, content, and applications on their network.

SAMPLE CUSTOMERS

Hyatt, ONS

TOP COMPARISONS

Fortinet FortiGate vs. Meraki MX Firewalls ... Compared 23% of the time [See comparison]
Cisco ASA vs. Meraki MX Firewalls ... Compared 19% of the time [See comparison]
Sophos UTM vs. Meraki MX Firewalls ... Compared 8% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Government ... 14%
Comms Service Provider ... 14%
Manufacturing Company ... 10%
Transportation Company ... 7%

COMPANY SIZE

1-200 Employees ... 51%
201-1000 Employees ... 19%
1001+ Employees ... 30%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 70%
201-1000 Employees ... 10%
1001+ Employees ... 20%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Meraki MX Firewalls

Top Reviews by Topic

💡 VALUABLE FEATURES

Phillip Peerman

The dashboard brings all management features with you wherever you are. All you need is an Internet connection and a browser and you can manage the solution. The dashboard tracks your uplink connectivity to the dashboard and double checks with you all changes impacting the connectivity, making it much safer to enact changes remotely. Dual WAN connections are greatly simplified and site-to-site VPNs automatically connect regardless of what WAN connection is active. Site-to-Site VPNs are the easier to setup than any other vendor's solution. You simple... [Full Review]

Rick Rutledge

The features we see and use the most are the SD-WAN, auto failover for dual ISP connections, auto failover for our VPN connections and the bandwidth monitoring are the main features. Alerting and monitoring are the next feature we see as being very beneficial. [Full Review]

Javier Jaime

* Managed centrally over the web: You can manages all your Meraki devices in a single account. * Site to Site VPN: The device can establish a VPN connection to multiple sites in a mesh environment in seconds, and without complex VPN knowledge. * Traffic Shaping: The device lets you decide how you want to use your internet services. Due to the fact that Meraki can accept dual WAN, you can decide the way you balance the data traffic. * Content Filtering: Excellent, and very easy to use. You can establish rules over specific content, what is allowed to... [Full Review]

Jeff Khan

AutoVPN features allow you extremely simple mesh or site to site IPSEC VPN tunnels with no configuration. It's self managed and saves a bunch of time and effort. Setup and configuration is cloud controller based so you just setup anything you need and don't actually have to configure the device other than to ship it to where it's going, and it configures itself with the settings you used without needing to hit the local LAN interface. [Full Review]

📄 IMPROVEMENTS TO MY ORGANIZATION

Phillip Peerman

* Easy of use * Remote management We are an MSP and Meraki provides MSPs with a combined management dashboard to centralize all clients under one single pane of glass. They offer a dynamic DNS, so Client VPNs and point-to-point VPNs can dynamically follow IP changes with no need for static IPs. The SD-WAN VPNs are also the easiest VPNs to setup in either a mesh or hub-and-spoke configuration that you will find. It works with non-Meraki VPN equipment too. [Full Review]

Rick Rutledge

As the only network admin in the company, I have to monitor nine remote sites (production and shipping facilities) and 12 remote VPN connections from various smaller facilities. Each location is a processing facility, which, when in season, runs 24 x 7 for the duration they are in production. During this time frame, not having a tech support person on site to fix problems is a huge cost savings for us. I see problems usually before they are large enough to need someone on site and with the cloud services I can remotely control ports, firewall connec... [Full Review]

Javier Jaime

Meraki lets us control all the traffic data and analyze it. The Traffic Shaping lets us install voice servers and give quality of service. It prevents us from being hacked and delivers information about who and where the attack came from. [Full Review]

Meraki MX Firewalls

ROOM FOR IMPROVEMENT

Phillip
Peerman

Some advanced enterprise features are missing, but for SMBs this solution is a dream to deploy and manage. Complex environments should look elsewhere, but I personally have not ran across anything that Meraki has not been able to handle so far. On the dashboard is a "Make a Wish" button to request new features. In three years, I have made three wishes and they were all were granted. [Full Review]

Jeff Khan

There are a few things that are odd that I can do with other firewall products that I can't do with a Meraki. Such as - wanting to setup two firewalls in front of the same protected subnet. Since they 'act' like one when they are added, it won't let you setup the firwall in the traditional way where it's on the same LAN and has a proper public IP. When you attempt to save, because of their oversimplification of firewalls, it complains that you already have a firewall in front of that subnet. The only choice the leave you is to match the exact firewa... [Full Review]

PRICING, SETUP COST AND LICENSING

Phillip
Peerman

Other content filtering solutions that I have used had more bells and whistles, but given the cost, complexity, and management overhead, I am very pleased with Meraki's solution. [Full Review]

Rick
Rutledge

Well, you get what you pay for. If you want good products that work well and are easy to configure, as well as remote control, you have to weigh the pricing options. Is it worth the extra few bucks? I think so. Meraki comes with a limited lifetime warranty and they will replace the failed unit overnight if one fails. [Full Review]

Javier Jaime

It is more expensive than other solutions, but it is a cloud-managed network solution and support is given at the moment you call. That give a very big plus. The Meraki UTM is excellent when you buy the Advanced Security license. If you buy a different license you lost all the valuable functions. [Full Review]

Frank
Theilen

Compare total costs (setup and management), taking in mind that cloud features do more than just stop traffic on the edge: they identify both traffic and users. [Full Review]

Sophos Cyberoam UTM

Overview

Cyberoam Unified Threat Management hardware appliances offer comprehensive security to organizations, ranging from large enterprises to small and branch offices. Multiple security features integrated over a single, Layer 8 Identity-based platform make security simple, yet highly effective.

SAMPLE CUSTOMERS

Gulf Corporation for Technology, Maridive & Oil Services, Fidelity Bank, Petra University, Capital FM Kenya, Safari Park Hotel and Casino, Mayfair Casino, Pacific International Lines, Mozambique Ministry of Education, University of Namibia, Royal Hospital for Neuro-disability, University of Hawai, New Delhi Municipal Council

TOP COMPARISONS

Fortinet FortiGate vs. Sophos Cyberoam UTM ... Compared 33% of the time [See comparison]
Sophos UTM vs. Sophos Cyberoam UTM ... Compared 14% of the time [See comparison]
SonicWall TZ vs. Sophos Cyberoam UTM ... Compared 12% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 13%
Comms Service Provider ... 9%
Non Tech Company ... 8%
Transportation Company ... 7%

COMPANY SIZE

1-200 Employees ... 38%
201-1000 Employees ... 35%
1001+ Employees ... 27%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Hospitality Company ... 8%
Non Profit ... 8%
Government ... 8%
Non Tech Company ... 8%

COMPANY SIZE

1-200 Employees ... 46%
201-1000 Employees ... 27%
1001+ Employees ... 27%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Sophos Cyberoam UTM

Top Reviews by Topic

💡 VALUABLE FEATURES

Chinyama Zama

For me, the web and content filtering are valuable because that, unfortunately, is where the abuse happens a lot. People are abusing the network and pushing up the bandwidth price. [Full Review]

Ersin Bostancɪ

The performance and security are the best features. The security options are great. We never had an attack, which is pretty good. We use it from a standard location, and they are connected to each other. [Full Review]

Muhammad Irfan

For me, the most important thing is content management and, obviously, the firewall because we have some servers. We have different levels of users. Some users, we are just giving them email access. For some users, working sites only. For some users, we are giving them intermediate access so they can access, on the government side, some knowledge bases. For some users, we are giving full access. So there are two major features for me. One is content management and the second thing is servers, publishing. [Full Review]

Abdul Faheem

The best feature is the flexibility the product offers, in terms of remote access. We have bout 35 locations across the kingdom, and connecting those remote locations with the minimal bandwidth was a challenge. A few of my branches are connected via 3G. So that is the most advanced feature I like about Cyberoam, the flexibility the solution offers. [Full Review]

📄 IMPROVEMENTS TO MY ORGANIZATION

Chinyama Zama

One of the benefits has been cost reduction because I am now able to monitor my bandwidth. I have just enough bandwidth to utilize within the organization, without having to spend significant amounts toward additional bandwidth. That has been one of the major benefits. It has also increased productivity within the organization because now, fewer people are spending time abusing the network, and are focusing more on their jobs. I have not totally blocked everything, they do get their social life after hours, it's just a control during work hours. [Full Review]

Fred Fish

The ability to have a site to site VPN, yet have the users use their local internet rather than sending all traffic back to our main site is crucial to their day to day operations. Remote VOIP phone system routing through the VPN we have extension connections to those remote campuses. [Full Review]

Muhammad Irfan

Before, I was using TMG, and it was very difficult, back in 2010. A lot of things, like HTTP filtering and HTTPS filtering, were a problem for me at the time. If someone asked me to block YouTube for example, I was able to do so in TMG but when it came to HTTPS, I was having some problems. So this is one issue we have resolved. The second issue, before the firewall, was we only published our required port on the internet. Third, email filtering. Before, because we were using Go Daddy services, just normal services for email, we had everything coming... [Full Review]

Sophos Cyberoam UTM

ROOM FOR IMPROVEMENT

Chinyama Zama

Once in a while, an unwanted email will slip in. You have to set your parameters to avoid that happening, but once in a while, an email has slipped past firewall. Once you update the firmware, you notice that it doesn't happen. If an email slips in, I get a little bit worried. I do get the report, but you just don't want that situation happening in the first place. When I look comparatively at certain products like Check Point - I haven't used Check Point but I have seen it in action - the people who have actually used it have confirmed that they ha... [Full Review]

Fred Fish

We have issues with IPS and DoS attacks taking down a couple of our sites. I've changed the IPs of the external interfaces yet the attacks still happen and the Firewall will disconnect the VPN connection as well as stop all internal traffic from flowing externally. I am still able to HTTPS to the external interface, but it takes a full reboot of the appliance to get any traffic flowing again. [Full Review]

Ersin Bostancı

I am not sure there will be a another release of Cyberoam because it will be Sophos going forward. What could be included going forward though? I would like to see a better content management pack and also the website searching should be better. [Full Review]

Muhammad Irfan

They have some issues with email filtering. Sometimes, I have found emails that have passed through the firewall, so I contacted Cyberoam. They said, "Okay, we are going to update the signature in the next update you, you will not get it like this again." [Full Review]

PRICING, SETUP COST AND LICENSING

Fred Fish

These, CR15iNG remote/small office firewalls, units are pretty inexpensive and renewal pricing is well worth the support cost. They do not have a hardware replacement support agreement at this time with Cyberoam. I do believe Sophos is changing that portion of the support agreement though. [Full Review]

SenSupAn8 49302

The hardware has no user limit (the hardware is the limit) while the virtual edition has user limits (I do not like limits). It is a bit expensive, but totally worth the money. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

WatchGuard XTM

Overview

Small businesses need big security, too, and the WatchGuard XTM Series firewall/VPN appliances deliver that strong protection Đ but without the hefty price tag. Enterprise-grade security includes full HTTPS content inspection, VoIP support, and optional security subscriptions like Application Control and Intrusion Prevention Service.

SAMPLE CUSTOMERS

AVG, Cyren, Kaspersky Lab, Lastline, NCP engineering, Trend Micro, Websense

TOP COMPARISONS

Fortinet FortiGate vs. WatchGuard XTM ... Compared 28% of the time [See comparison]
Sophos UTM vs. WatchGuard XTM ... Compared 14% of the time [See comparison]
SonicWall TZ vs. WatchGuard XTM ... Compared 11% of the time [See comparison]

REVIEWERS *

VISITORS READING REVIEWS *

TOP INDUSTRIES

Comms Service Provider ... 13%
Financial Services Firm ... 8%
Manufacturing Company ... 7%
Transportation Company ... 7%

TOP INDUSTRIES

Financial Services Firm ... 36%
Healthcare Company ... 14%
Logistics Company ... 14%
Local Government ... 7%

COMPANY SIZE

1-200 Employees ... 44%
201-1000 Employees ... 31%
1001+ Employees ... 25%

COMPANY SIZE

1-200 Employees ... 72%
201-1000 Employees ... 22%
1001+ Employees ... 6%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

WatchGuard XTM

Top Reviews by Topic

VALUABLE FEATURES

Somono Chek

The proxy based policy in Policy Manager is the best feature. It helps me: * Create many different firewall policies for different networks and services * In tracking problems in the policy rule in the traffic monitor of Firebox System Manager [Full Review]

DirSec3509

The most valuable features of the solution are the subscription services that come with the product: * Intrusion Protection - This is pretty standard across all products. * WebBlocker - It used to be called WebSense. For a decent-sized organization that's a $200,000 product, and we get a fully-implemented version of that inside our product. * Data Loss Prevention - This feature is really good for sorting out the loss of credit card information or other valuable information. * Application Control - This is fantastic with over 2,500 applications and t... [Full Review]

Gevorg Harutyunyan

Packet filters and proxy policies are valuable features. They allow you to configure restrictions by domain name. These features are useful to block web pages which have multiple IP addresses, such as Facebook. [Full Review]

Paal

Ease of setup. All WatchGuards are pretty much the same to setup and manage. We experienced that WatchGuard is easy to setup regarding VPN compared to other firewalls of other brands. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

Somono Chek

With this product, I can easily block group websites with its WebBlocker based on predefined categories such as: Social Network, Sex Material, and Video Streaming We can also use Application Control to block some applications based on pre-defined categories such as: P2P, Social Network, Streaming Media, and Games. [Full Review]

Gevorg Harutyunyan

It was installed as two redundant XTM 850s (active-passive). The XTM 850s perform as a general firewall and as a filter of WAN traffic. Routers are configured as a load balancer for internal VLANs and for WAN as well. Other network functionality is based on Extreme Networks equipment. [Full Review]

Alexander Padilla

Security is a requirement for any organization, using WG products you can deploy faster solutions to big problems with a fair price. Based on WG, we can deploy 30 offices in a few days, and maintain an excellent visibility of the network traffic for the entire network, using a single console. [Full Review]

WatchGuard XTM

ROOM FOR IMPROVEMENT

Somono Chek

1. It is difficult to configure WatchGuard with your internet settings. Actually, a normal internet setting/configuration is easy. However, I had a problem with multi WAN and multi LAN. I have a few different LAN subnet and two WAN. What I want to do is to route traffic from LAN1 through WAN1 and use WAN2 as failover. And for LAN2, it would route through WAN2 and use WAN1 as failover. So all traffic from LAN1 supposed to go through WAN1 only unless WAN1 is down, then it will go WAN2. However, I still could see some packet from LAN1 go through WAN2 a... [Full Review]

Gevorg Harutyunyan

The management console and web interface are very bad. They should improve it and add more command lines and easy scripting functionality. I also suggest adding/improving smart and easy logging and debugging tools. [Full Review]

Paal

Client-based administrative tool. Cloud-based central administration of all devices from one point would be nice (although there is always an added risk regarding this). [Full Review]

Jhon Perez

Licensing should be improved. It should allow you to keep the rules that are created; at the end of the grace period, it does not allow you to create new rules but only to maintain the current ones. The mobile administrative management applications (mobile devices) should be improved. [Full Review]

Juniper SRX   See 14 reviews >>

Overview

High-performance security with advanced, integrated threat intelligence, delivered on the industry's most scalable and resilient platform. SRX Series gateways set new benchmarks with 100GbE interfaces and feature Express Path technology, which enables up to 1 Tbps performance for the data center.

SAMPLE CUSTOMERS

7-Eleven, AARNet Pty Ltd, Allegro Networks, alltours GmbH, Apollo Hotel Papendrecht, Armstrong Atlantic State University, Atlantech Online, Availity, Bajaj Capital, Baloise Insurance, BancABC, BAS Group, Black Lotus, Blue Box, Borealis, Carilion Clinic, Catholic Health System, CATV, Champlain College, China⊡s Ministry of Railways, China University of Mining and Technology (CUMT), Cloud Dynamics, CloudSeeds, Cloudwatt, CODONiS, Colt Technology Services, Cork Internet Exchange, CSS Versicherung AG, CyrusOne, Danish Crown, Deloitte Belgium, Department of Energy, Divona Telecom, DQE Communications, DreamHost, European Government Agency, Expedient, Financial Market Information Services Provider, Fluidata, Fonality, Fox Sports, Global Financial Institution, Global Investment Bank, Global Investment Company, Energy Sciences Network (ESnet), Goethe University, HEAnet, High Performance Networks Inc., Hillenbrand

TOP COMPARISONS

Fortinet FortiGate vs. Juniper SRX ... Compared 31% of the time [See comparison]
Cisco ASA vs. Juniper SRX ... Compared 23% of the time [See comparison]
Palo Alto Networks WildFire vs. Juniper SRX ... Compared 10% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Comms Service Provider ... 25%
Marketing Services Firm ... 13%
Manufacturing Company ... 12%
Financial Services Firm ... 8%

COMPANY SIZE

1-200 Employees ... 32%
201-1000 Employees ... 49%
1001+ Employees ... 20%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Comms Service Provider ... 38%
Financial Services Firm ... 25%
Retailer ... 13%
Energy/Utilities Company ... 13%

COMPANY SIZE

1-200 Employees ... 37%
201-1000 Employees ... 21%
1001+ Employees ... 42%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Juniper SRX

Top Reviews by Topic

VALUABLE FEATURES

Se32Ntwk2190

I'm not sure what the most valuable features are. I'm not really that impressed with the technical support. I'm not really that impressed with the product, to be honest with you. Throughput seems to be okay. [Full Review]

Roger Bascom

* I am really hesitate to repeat the Juniper sales line of "One Juniper", simply because within different devices, there are differences in the CLI commands used. This has been due to functional and hardware differences. For the vast majority of the Juniper CLI commands, if you learn them for the SRX, they are the same for the EX and QFX series switches. There is little to no differences between the Junos OS versions * The "candidate configuration" and rollback features are real life savers. They are different from what Cisco does. At a Cisco CLI, w... [Full Review]

Charles Ogwari

* Form factor: It is small, very nimble, and can be deployed in very small environments which do not have wiring closets. * Consolidation: It combines routing, switching, and firewall services in one device. * Stable OS: There is a one Junos release training for all the Juniper products, thus minimizes the training needed and enhances interoperability. * Open standards: The Juniper OS is based on the open standards and making it very interoperable in the mixed vendor environments. * Superior performance: This can be achieved by true separation of co... [Full Review]

Leke Oluwatosin

Valuable features for us include: * Routing: When firewalls can also perform full routing functionality, it helps to save cost on dedicated routing hardware. * High Availability (clustering): This is important to ensure service availability in the event of a node failure. These firewalls in HA mode consist of a primary and backup node, and provide redundancy such that if one of the nodes fails, the other node will take over. * Deep packet inspection (DPI) capabilities: Juniper SRX firewalls inspect packets as they traverse the firewalls and it goes ... [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

Se32Ntwk2190

The Juniper was a later model, later technology than we had, more horsepower than we had before. The performance is better, but it could have been any firewall in its peer group. The improvement was because our old firewalls were, well, old. So the performance has been an improvement. And the IDS, perhaps, is a little better than what the older firewalls had. [Full Review]

Roger Bascom

* Once our engineers got their heads wrapped around the nuances of Juniper's CLI and are function on par with them. I recommend investing in Juniper Space if you have a significant amount of Juniper equipment to manage. We have three of the larger SRX550s, with one cluster configuration, for edge security devices. We are very happy with them. * Not specifically in SRX category, but the 40Gb/10Gb interfaces in the QFX gear are truly wired for speed on all available ports. The virtual EX switch chassis configuration, where up to 10 switching devices c... [Full Review]

Charles Ogwari

It has greatly reduced the network management functions by reducing the number of devices to manage (one vs three), and easy fault management using the new GUI. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

Juniper SRX

ROOM FOR IMPROVEMENT

Se32Ntwk21 90

The CLI is verbose. You have to say a lot to do a little. I don't like that part of it. Cisco's command syntax seems to be a good bit more concise. When you're trying to get something done, you don't want to have to type a bunch. I wish there was a quicker way to configure through the CLI. I know all the tricks of hitting spacebar etc. to finish the command, and the context tricks of going further in. But it just reminds me of an older operating system, like VAX/VMS. It's just very verbose. Maybe this is where the Space Security Director product com... [Full Review]

Roger Bascom

Third-party support for Juniper is a lot less than Cisco. This is no surprise, but a definite consideration if you are expecting to use a lot of third party support. In my guesstimate, for every 100 Cisco shops, you will find one Juniper shop. [Full Review]

Ales Ciber

Web management needs to improve. The web interface on Juniper SRX is just a short conversion from Junos OS CLI; this is not very suitable for users with little expertise. But Juniper has complete MGMT for managing SRX devices and other Juniper devices. it's called Junos Space with APP security director for security devices. It's good, but there is space for improvment. [Full Review]

Jean Almeida

It would be good if Junos had "unique commands" between all hierarchical levels, discarding the use of the "Run" command. The robustness of Linux on top of Junos can be more effective after power down. [Full Review]

PRICING, SETUP COST AND LICENSING

Charles Ogwari

The price per performance value is the best out there in the market. No licensing is needed for all the features apart from the security part, i.e., no licensing for extra services and VPN comes free in the base. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

SONICWALL **SonicWall TZ**   See 7 reviews >>

Overview

The secure, sophisticated SonicWALL TZ is widely deployed at small businesses, retail, government, remote sites and branch offices. It combines high-performance intrusion prevention, malware blocking, content/URL filtering and application control.

SAMPLE CUSTOMERS

AeroM_xico Delta TechOps, Unimat

TOP COMPARISONS

Fortinet FortiGate vs. SonicWall TZ ... Compared 30% of the time [See comparison]
Cisco ASA vs. SonicWall TZ ... Compared 11% of the time [See comparison]
WatchGuard XTM vs. SonicWall TZ ... Compared 10% of the time [See comparison]

REVIEWERS *

VISITORS READING REVIEWS *

TOP INDUSTRIES

Marketing Services Firm ... 13%
Manufacturing Company ... 9%
Financial Services Firm ... 8%
Transportation Company ... 7%

COMPANY SIZE

1-200 Employees ... 75%
201-1000 Employees ... 25%

COMPANY SIZE

1-200 Employees ... 43%
201-1000 Employees ... 31%
1001+ Employees ... 26%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

SONICWALL SonicWall TZ

Top Reviews by Topic

☀ VALUABLE FEATURES

Lucius Quarshie

We use the content filter quite a lot because it's an office setting. During working hours, we like to censor the sites users can visit so it increases productivity. Therefore, the content filter has been good for us. We have been using the SSL VPN as well, because most of our people do travel. They go for rest and recuperation approximately every six weeks, and they are offsite for about 10 days. More often than not, they need to login, or get onto shared drives, to do some work. [Full Review]

GustavoVila Verde

SonicWALL TZ has a lot of great features. For me, the best features are Application Control and Sandbox. We could deny or allow any applications because the firewall works in Layer-7. In the sandbox, the network files are tested and validated to make sure the file are clean. This increases the security. [Full Review]

Darrel Harvey

I really don't know. I'm not really an IT person, per se, but I would say number one is the protection available, and then ease of use and flexibility. Those would be the top three. [Full Review]

📖 IMPROVEMENTS TO MY ORGANIZATION

Lucius Quarshie

We use the content filter and the SSL VPN: * The content filter has increased our productivity, especially during working hours. We don't have users spending time on social media during working hours. This means productivity is good. * Then, when the guys are offsite, they are still able to work without taking any breaks due to the SSL VPN that we use. [Full Review]

Aaron Krytus

The site-to-site VPN allows for consistent communication between sites. Upgrading the OS is easy and they alert you when an upgrade is available. Content filtering and gateway security has help reduce visiting unwanted websites and attacks. Logging helps track down issues bandwidth hogs. [Full Review]

GustavoVila Verde

This solution is very good in terms of its security and its productivity. The feature that helps many companies the most is Bandwidth Control, as this increases the users' productivity. [Full Review]

reviewer471 591

We have several locations, each with a VPN to a central office. SonicWall provides each location with its own security and provides our company with the ability to centralize our servers so they can provide applications to all the locations and users. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

SonicWall TZ

ROOM FOR IMPROVEMENT

Lucius Quarshie

SonicWall Analyzer needs a different license. It would be good if Analyzer would be part of the stock license, so even if a layperson is getting the device, he or she doesn't forgets about ordering the Analyzer because it's already there. This is what we realized that over the last few months. We tried to pull some analysis, and without the Analyzer, we couldn't. Now, we are in the process of buying the additional license. It would have been better embedded from the beginning. [Full Review]

GustavoVila Verde

* Increase SSL connections and reports. * The SSL connection is based on the amount of the user throughput. When this feature is enabled in any player of the Firewall, the hardware has a lot of work to do * The reports are great when a report is needed about security, viruses, Botnet, VPN, attacks, etc. But the user websites report is not too clean. I think it could be improved. [Full Review]

Darrel Harvey

I'm not an IT guy. What I will say is that the market seems to be going to a cloud-supported, new generation of firewall products. I think that's probably going to be important to us, the next time around. [Full Review]

Bruce Bower

I would like them to make the interface a little bit easier to use so you can find out where in the heck you're going instead of having to go to 15 different places to get something installed. [Full Review]

PRICING, SETUP COST AND LICENSING

Lucius Quarshie

SonicWall has authorized distributors in our country. They have about two or three distributors in the country, so it makes it a bit easier. What we do is to request a quotation from these distributors, then we do a value for money analysis and see which one of them is giving us a competitive price. Getting licenses in our country, Ghana, is not easy. Though, once we have them, adding them is quick (about a day). Overall, the cost is great. [Full Review]

Aaron Krytus

Sonic Wall has an a la carte pricing model. There are many features and options that you may not need or want and therefore no need to pay for them The only problem with this model is that it does now use a yearly subscription model. Although the router itself may be less expensive than other competitors, you may spend more in subscriptions. Product support will require a yearly maintenance. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

SonicWall NSA

Overview

Achieve a deeper level of security with the SonicWALL Network Security Appliance (NSA) Series of next-generation firewalls. NSA Series appliances integrate automated and dynamic security capabilities into a single platform, combining the patented, SonicWALL Reassembly Free Deep Packet Inspection (RFDPI) firewall engine with a powerful, massively scalable, multi-core architecture. Now you can block even the most sophisticated threats with an intrusion prevention system (IPS) featuring advanced anti-evasion capabilities, SSL decryption and inspection, and network-based malware protection that leverages the power of the cloud.

SAMPLE CUSTOMERS

Orange County Rescue Mission, First Source, Michaels & Taylor, Green Clinic Health System, Aspire Chiltern Skills and Enterprise Centre, UnitedStack, Faith Lutheran College Redlands, Celtic Manor Resort, Star Kay White, Air Works, Unimat Life, NHS Yorkshire and Humber Commissioning Support (YHCS), Hutt City Council, Mato Grosso do Sul, Nspyre

TOP COMPARISONS

Fortinet FortiGate vs. SonicWall NSA ... Compared 23% of the time [See comparison]
Sophos XG vs. SonicWall NSA ... Compared 12% of the time [See comparison]
Meraki MX Firewalls vs. SonicWall NSA ... Compared 12% of the time [See comparison]

REVIEWERS *

VISITORS READING REVIEWS *

TOP INDUSTRIES

Writing And Editing Position ... 16%
Transportation Company ... 12%
Construction Company ... 12%
Manufacturing Company ... 10%

COMPANY SIZE

1-200 Employees ... 67%
201-1000 Employees ... 25%
1001+ Employees ... 8%

COMPANY SIZE

1-200 Employees ... 56%
201-1000 Employees ... 31%
1001+ Employees ... 13%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

SonicWall NSA

Top Reviews by Topic

VALUABLE FEATURES

adoughe

I like that you can run a packet capture from within SonicWall and configure it to automatically upload the packet captures to an FTP server. This is useful when trying to troubleshoot an intermittent issue. It can capture for as long as you have disk space on the FTP server. [Full Review]

Leen Van Gent

At the moment, none. It just doesn't do its task. Users, no matter how you configure it - and it's configured quite carefully in the sense of censoring - seem to be able to punch to the file. It just doesn't do its job. It seems to have all the features, it's just not performing. It has good reporting, the reporting is marvelous, but reporting is always after the fact and you want to be proactive if you're a firewall. You don't want to be saying "Ah! We had a bot running on the network," while SonicWall itself didn't give that indication in an activ... [Full Review]

Steven SL.

Application control: It allows us to block applications, i.e., websites by application type category. It is far more capable than content filtering alone. [Full Review]

Michael D'Antignac

Because this is a UTM, we appreciate having a single pane of glass for a firewall, content filtering, and IPS/IDS services. It is much easier to manage and costs less. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

adoughe

We are more aware of security issues since SonicWall can be configured to send e-mail alerts. Server-side Outlook rules and Exchange transport rules (more informational subject lines) can be helpful in sorting and making sense of the many alerts it can generate. We have also configured it to send logs to a syslog server. They also offer SonicWall Analyzer which can reportedly be very helpful when viewing logs but I have no experience with it. [Full Review]

Steven SL.

For the average SMB, this firewall does the job quite well. Granular user controls, firewall and NAT rules that you would expect. Licensed features provide application control, content filtering, antivirus, and anti-malware all in a single appliance. [Full Review]

Michael D'Antignac

In a K-12 environment, internet security is paramount and threats change quickly. The main improvement for the organization is uptime and the ability to quickly affect security changes. The second plus is the ability to improve throughput during peak traffic hours. [Full Review]

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

SonicWall NSA

ROOM FOR IMPROVEMENT

adoughe

I am not sure if SonicWall has finally addressed this issue but a major area for improvement would be being able to export the settings file in a non-binary readable and editable format. It is not possible to export, make changes and then upload a revised configuration. Since the settings file is binary and non-readable, it seems to always be suspect when any strange issues arise with the appliance. I have had their techical support many times through the years question whether our settings file was corrupt. Of course it would be very easy to know i... [Full Review]

Leen Van Gent

The problem primarily with SonicWall is it's a Unix box. And it's all software, all the activities, blocking, censoring, everything has to happen in the software. If you start hitting the box with a lot of sessions it slows down and that's not what I expect from a firewall. I have worked with this box for six months, and it's a daily task to manage this thing. You don't have to always have time to do this. The room for improvement is to step away from the Unix platform. It needs to be a specialized system that manages firewall activity. You don't wa... [Full Review]

Steven SL.

SonicWall has weaknesses. During its tenure with Dell, it was severely damaged. VPN: Site-to-site is solid! Client-based VPN is another hot mess. Global VPN client issues and mobile connect issues. Do not even consider NetExtender - probably one of the most horrific, nightmare grade Java-based VPN clients. We have but all given up trying to make it work reliably. [Full Review]

Michael D'Antignac

SonicWall uses a cloud-based database for content filtering. If the NSA cannot contact that online DB, filtering is handled one of two ways. Traffic is either halted completely or it is passed-through totally unfiltered. In a K-12 school environment, neither is acceptable. It would be better if the DB can reside on the NSA and is used in the event the online DB is unavailable. Other than that, it works fine. [Full Review]

PRICING, SETUP COST AND LICENSING

adoughe

SonicWall absolutely has the best bang for the buck hands down. Other firewalls are two to three times as expensive both in initial cost and recurring maintenance cost. SonicWall does not require duplicate licenses if you have an HA-pair in Active/Passive mode since only one unit will be active at any given time, which is a big savings in cost compared to other vendors. If you buy a security bundle you get even greater savings. SonicWall does, however, license user VPN access unlike most other vendors. [Full Review]

Kevin Cabrera

SonicWall's Next Generation Firewall itself, I believe, is not expensive for the features and the protection it offers. Though the licensing is the big problem, especially for those companies with flat budgets for IT. My advice would be for everyone to avail themselves of at least three years of licensing to save tons of money. [Full Review]

Answers from the Community

How do you plan for a security review for firewalls?

Is it required in your company to conduct a security review before purchasing a firewall? What are the common materials you use in the review? Do you have any tips or advice for the community? Any pitfalls to watch out for?

Chris Loehr

If you are a small shop, you need to trust your MSP, VAR or another reseller when purchasing a firewall. Don't just go online and buy direct. Resellers have trained people. Most mainstream vendors even have devices that can be deployed ahead of time to get a good idea of your firewall needs. In today's firewall world, it comes down to the software package that you license on your firewall. If you get a firewall without the security software, you are not getting an effective firewall. If you a midmarket or large company, there are tools such as ThreatCare that can help you test the effectiveness of the firewalls your are putting through proof-of-concept testing. They will test how well the capabilities are working, especially the ones that are in place to ensure confidential information does not go out of your network without authorization.

Dan Stolts

Yes, I recommend doing a security review regularly. Not necessarily before a firewall purchase unless you have not done one lately. Having the results of the review will help you understand what capabilities you need in a firewall. As an example, if you get a ton of login attempts from outside your country of origin but have no customers or partners outside the country you will want to have "country blocking" capabilities. There are a number of tools that can be used for evaluations. We currently use RMM and Security tools from SolarWinds. We have other tools as well. To perform a security review you have to have tools do the work. It simply is not possible for an individual to perform a thorough check without significant automation. We offer this as a service as well. Pro's: SolarWinds has a free version of some of the useful tools such as...

Michael Majeski, Mba,Pmp, Csm

Is it required in your company to conduct a security review before purchasing a firewall? Firewalls review are usually done annually and equipment is purchased to protect each network data point What are the common materials you use in the review? To verify the open ports, services, and applications of what is allowed and disallowed. Most companies are moving towards software like TUFIN to help continually perform these rule deployments and changes globally. Do you have any tips or advice for the community? Adapt to a common service platform to connect to service desk, deployments and regular review to reduce errors and service time to deploy FW changes. Any pitfalls to watch out for? Not being able to survey automatically current FW rules and settings could leave the company vulnerable to intrusion or failed services for internal stakeholders.

[See all 20 answers >>](#)

To read more reviews about Firewalls, please visit: https://www.itcentralstation.com/categories/firewalls

About this report

This report is comprised of a list of enterprise level Firewalls vendors. We have also included several real user reviews posted on ITCentralStation.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About IT Central Station

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created IT Central Station to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

IT Central Station helps tech professionals by providing:

- A list of enterprise level Firewalls vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use IT Central Station to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

IT Central Station

244 5th Avenue, Suite R-230 • New York, NY 10001
www.ITCentralStation.com
reports@ITCentralStation.com
+1 646.328.1944