UTM

(55 قسمت) آموزش رایگان دوره Network+ (شبکه)

قسمت قبل

در قسمت قبل آموزش رایگان دوره **(Network+)** شبکه

Internet
Firewall
Private network

در شکل زیر تجهیزات امنیتی و دیوارهای آتش سختافزاری را مشاهده میکنید که برای حفاظت از یک شبکه متوسط یا بزرگ استفاده میشوند .

Search Results - Showing 73 - 96 of 215 Products

Sold by: ☐ Newegg only

Sort: Lowest Price

View: 24

Type : Wired

NeweggBusiness - Netw
neweggbusiness.com/product/productlist.aspx?submit=ene&n=100022143%20600030409&isnodeid=1&name=w
NARROW RESULTS
Power Search ▶
Manufacturer
☐ SonicWall (524)
☐ Cisco Systems, Inc. (165)
☐ WatchGuard (144)
☐ Ubiquiti Networks (12)
☐ Fortinet Inc. (33)
☐ ZyXEL (69)
Type
☑ Wired (1051)
☐ Wireless (355)
☐ Wired + Wireless (215)
Search Within
Go
Reset
Includes 3 Year Energize Updates
FREE SHIPPING
☐ Compare
Barracuda F18 Network Security/Firewall Appliance
☐ Compare
ZyXEL USG110-GB0102F Firewall Appliance
FREE SHIPPING
☐ Compare
Fortinet FortiGate Rugged 30D Network Security/Firewall Appliance

لازم به توضیح است که شما برخی از ویژگیهای یک دیوارآتش را روی دستگاههایی همچون روترها، سوئیچها و سایر دستگاههای شبکه در اختیار دارید . دقت کنید عملکرد همه دیوارهای آتش یکسان نیست. بهطور مثال، یک دیوارآتش مبتنی بر میزبان تنها از کامپیوتری که روی آن نصب شده است محافظت میکند .

نکته امتحانی : انواع مختلفی از دیوارهای آتش وجود دارند و میتوان آنها را به روشهای مختلفی پیادهسازی کرد . برای درک نحوه طراحی یک شبکه امن و موفقیت در آزمون نتورکپلاس باید به خوبی این مسئله را بدانید که دیوارهای آتش میتوانند چه کارهایی انجام دهند، در چه بخشی از شبکه قرار میگیرند و چگونه باید ویژگیهای مورد نیاز خود در یک دیوارآتش را تشخیص دهید .

سادهترین شکل یک دیوارآتش، یک دیوارآتش فیلترکننده بستهها است که یک دستگاه یا برنامه تحت شبکه است که سرآیند هر بسته دادهای دریافتی از رابطهای مختلف (ترافیک ورودی) را آزمایش میکند . شکل زیر این مسئله را نشان میدهد .

Internet
Inbound
Outbound
Gi0/0
External
interface
Gi0/1
Internal
interface
Outbound
Inbound
Private LAN
Packet-filtering
firewall

[illegible]

[illegible]

[illegible]

- [illegible]

- [illegible]

- [illegible]

- [illegible]

[illegible]

- [illegible]

- [illegible]

- [illegible]

- [illegible]

- [illegible] OSI [illegible]
  [illegible]

- [illegible] IDS [illegible] IPS [illegible]

- [illegible]

- [illegible] (stateful firewall) [illegible]
  [illegible].

[illegible] SOHO [illegible] Fortinet [illegible]. [illegible]
[illegible]. [illegible]....[illegible] [illegible]
[illegible] iptables [illegible] ZoneAlarm [illegible] Comodo Firewall [illegible]
[illegible]. [illegible] 10 [illegible].

Unified Threat Management

[illegible] **Unified Threat Management** [illegible] (UTM) [illegible]
[illegible]. [illegible]
[illegible]. [illegible]
[illegible].

Intrusion Detection System

پویش ترافیک شبکه به بهترین شکل استفاده شوند .

سامانه های تشخیص نفوذ بر مبنای معماری به سه گروه NIDS، HIDS و DIDS تقسیم میشوند.

- **HIDS** (سیستم تشخیص نفوذ مبتنی بر میزبان) روی یک کامپیوتر واحد اجرا میشود تا حملات به یک میزبان را شناسایی کند . بهطور مثال، HIDS ممکن است تلاش برای بهرهبرداری از یک برنامه غیرایمن که روی یک سرور در حال اجرا است یا تلاشهای مکرر برای ورود به سرور را شناسایی کند . راهحل HIDS همچنین ممکن است شامل نظارت بر یکپارچگی فایل (FIM) سرنام file integrity monitoring باشد که سیستم را از وجود هرگونه تغییری در فایلهایی که نباید تغییر پیدا کنند همچون ویرایش فایلهای سیستمی آگاه میکند .

- **NIDS** (سیستم تشخیص نفوذ مبتنی بر شبکه) برای محافظت از یک شبکه یا بخشی از یک شبکه استفاده شده و معمولا در لبه شبکه یا در یک محیط محافظت شده شبکه که منطقه غیرنظامی (demilitarized zone) نام دارد نصب میشود. در اینجا، سامانه فوق میتواند انواع مختلفی از الگوهای ترافیکی مشکوک همچون حملات انکار سرویس یا حملات smurf را شناسایی کند .

- **DIDS** (سامانه تشخیص نفوذ توزیع شده) این سامانهها ترکیبی از دو مکانیزم قبلی همراه با یک ایستگاه مدیریت مرکزی هستند . در این مکانیزم هر سیستم تشخیص نفوذ موجود در شبکه گزارش خود را برای یک ایستگاه مدیریت مرکزی ارسال میکند . ایستگاه مرکزی نیز گزارشهای دریافتی را ارزیابی کرده و اگر مورد مشکوکی را پیدا کند، هشداری برای مسئول امنیت سیستم ارسال میکند .

در شماره آینده آموزش نتورکپلاس مبحث فوق را ادامه خواهیم داد .

نویسنده :
حمیدرضا تائبی
دسته بندی:
فناوری شبکه
تاریخ انتشار :
11:15 - 07/03/1398

برچسب:
آموزش رایگان شبکه - دوره رایگان نتورک پلاس - دوره نتورک پلاس - آموزش نتورک پلاس - آموزش رایگان دوره نتورک پلاس - آموزش دوره نتورک پلاس - آموزش رایگان Network+ - +Network - امنیت شبکه - امنیت در طراحی شبکه - دیوارهای آتش - Intrusion - Next Generation Firewalls - Unified Threat Management - Detection System - آموزش رایگان Network+

نشانی
□□□□:https://www.shabakeh-mag.com/networking-technology/15439/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-%D8%A8%D8%AE%D8%B4-55