



Firewalls

Modul D3.2

Referent: Dr. Jörg Cosfeld

Firewalls

Firewalls

Wer hat eine Firewall zuhause?

Firewalls

Wer hat eine Firewall zuhause?

AVM FritzBox 7490 VDSL DSL 100 50 WLAN Internet Router Modem für alle Anbieter NEU
★★★★★ 1 Bewertung



272,99 €

inkl. MwSt.

Kostenloser Versand

 In den Warenkorb

Firewalls

Sophos XGS 2100 - Sicherheitsgerät - GigE - 1U

SOPHOS



[Noch keine Bewertung](#)



Allgemein

Gerätetyp

Sicherheitsgerät

Höhe (Rack-Einheiten)

1U

Integrierte Peripheriegeräte

Status-LCD

Breite

43.8 cm

Tiefe

40.5 cm

Höhe

4.4 cm

Gewicht

4.7 kg

Lokalisierung

Großbritannien, Europa

[Alle Produktinfos](#)

3.211,50 €

Kostenloser Versand

Kostenlose Rücksendung innerhalb von 14 Tagen

1



In den Warenkorb

Kunstakademie Düsseldorf

Firewalls

Beispiele

Hochschule Düsseldorf

Palo Alto Networks PA-5280 Firewall System bis 68 Gbps, 64 Mio Sessions, 2x AC Netzteil [PAN-PA-5280-AC]



228.318,24 € *

zzgl. 19% MwSt. i.H.v. 43.380,47 €

Bruttopreis: 271.698,71 €

versandkostenfreie Lieferung Innerhalb Deutschlands ab 150 Euro

● Lagerbestand: 0 | Lieferzeit bis zu 60 Werktage

Kauf auf Rechnung / Firmenlastschrift? » [Mehr Infos hier](#)

1



In den Warenkorb



 Konfiguration speichern

 Merken

Artikel-Nr.:

PAN-PA-5280-AC

Firewalls

Rückblick auf Angriffsvektoren:

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff
- Aktiver Angriff

Firewalls

Rückblick auf Angriffsvektoren:

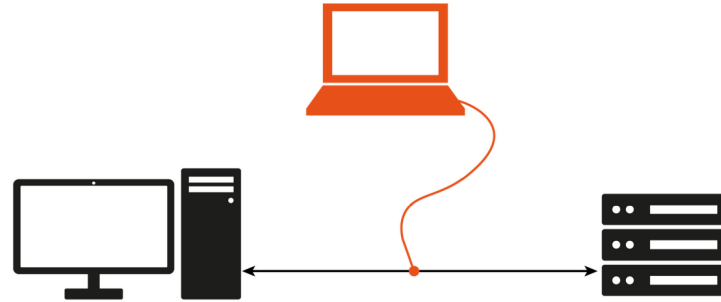
- **Passiver Angriff**

Abhören von Daten

- Aktiver Angriff

Angreifer gelangt in den Besitz von Daten

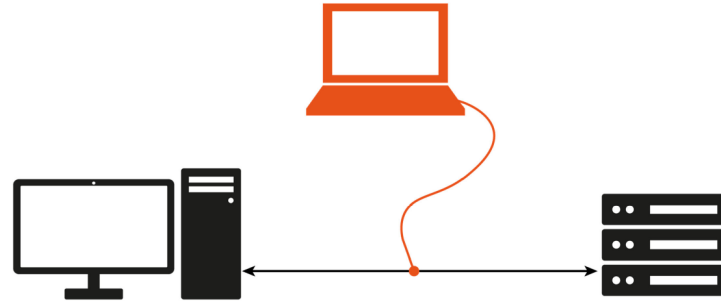
Angreifer schaltet sich zwischen die zwei Endpunkte der Kommunikation.



Firewalls

Rückblick auf Angriffsvektoren:

- **Passiver Angriff**



Abhören von Daten

- Aktiver Angriff

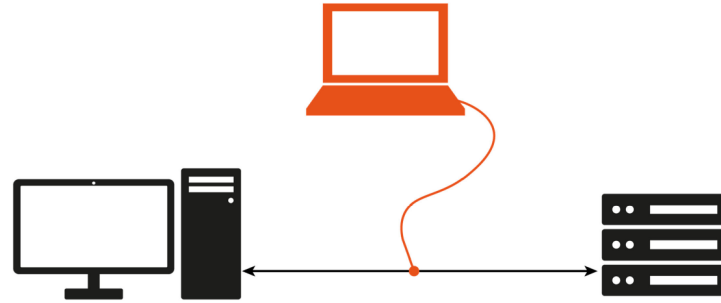
Wer tauscht mit welchem System Daten aus?

Wann wird eine Waschmaschine auf gekauft
und von welchem User?

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff



Abhören von Daten

- Aktiver Angriff

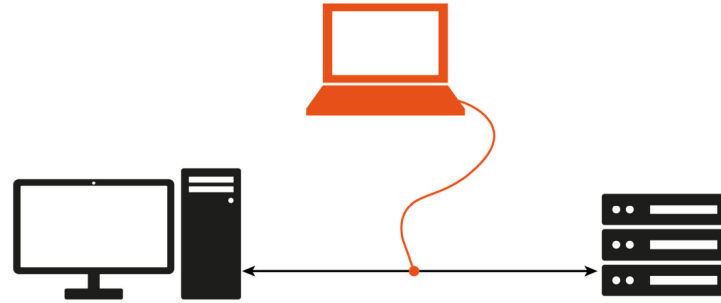
Wer tauscht mit welchem System Daten aus?

Wann wird eine Waschmaschine auf gekauft und von welchem User?

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff



Abhören von Daten

- Aktiver Angriff

Wer tauscht mit welchem System Daten aus?

**Faktor Mensch –
Phishing**

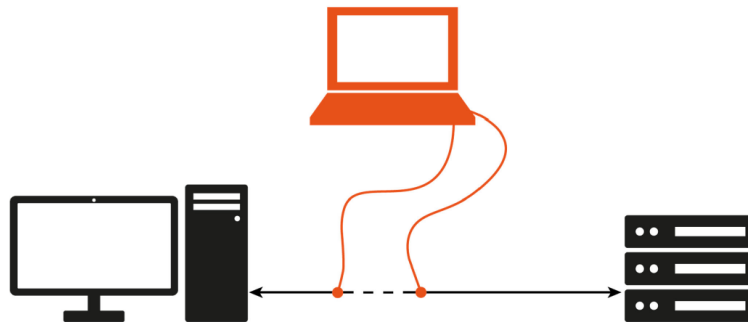
**Wann wird eine Waschmaschine auf gekauft
und von welchem User?**

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff

- Aktiver Angriff



Wiederholen, Blockieren oder Verzögern
von Information:

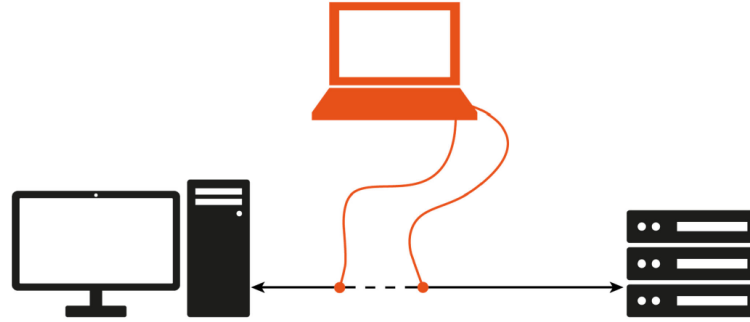
- Mehrfache Überweisung eines Geldbetrages
- Wiederholung eines mitgelesenen Logins

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff

- Aktiver Angriff



Manipulation der Daten:

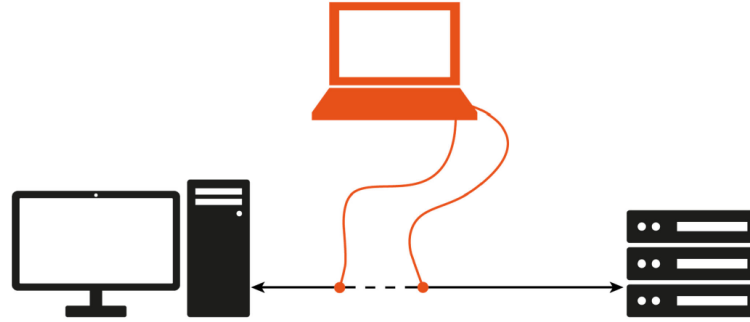
- Löschen oder Einfügen von bestimmten Informationen
- Geldbetrag auf der Überweisung wird geändert, oder sogar die Kontonummer

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff

- Aktiver Angriff



Denial of Service:

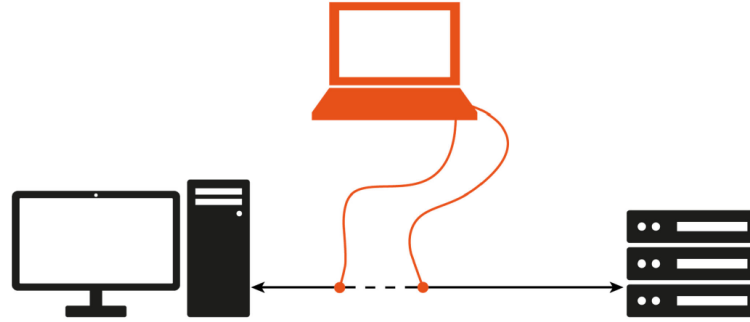
- Umfang der eingefügten Daten zu umfangreich.
- Server lehnt weitere Kommunikationen ab um sich zu schützen.

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff

- Aktiver Angriff



Man in the Middle:

- Mitlesen der Daten, Manipulation der Daten aus einem Wegepunkt in der Mitte
- Knotenpunkte wie Router werden genutzt

Firewalls

Rückblick auf Angriffsvektoren:

- Passiver Angriff
- Aktiver Angriff

Man in the Middle:

- Mitlesen der Daten, Manipulation der Daten aus einem Wegepunkt in der Mitte
- Knotenpunkte wie Router werden genutzt

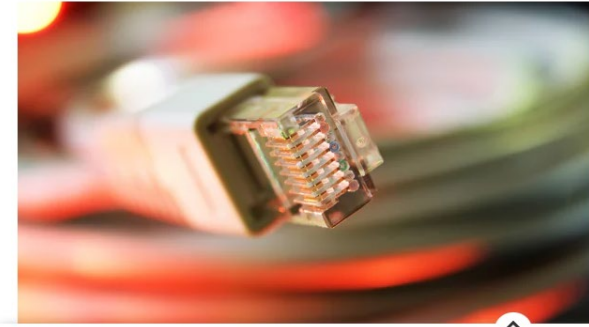
Alert!

Aruba: Kritische Sicherheitslücke in Access Points

Aruba warnt vor kritischen Sicherheitslücken in den eigenen Access Points.

Lesezeit: 3 Min. In Pocket speichern

🔊 🖨️ 💬 2



Firewalls

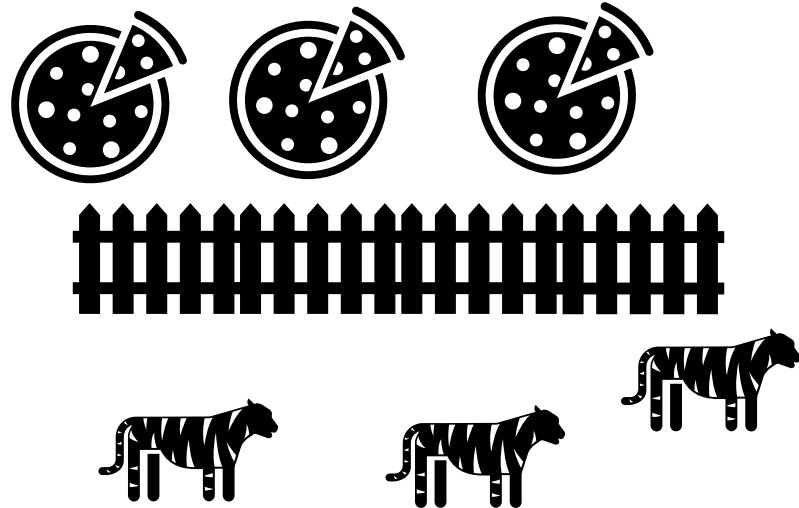
Definition:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

Firewalls

Definition:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

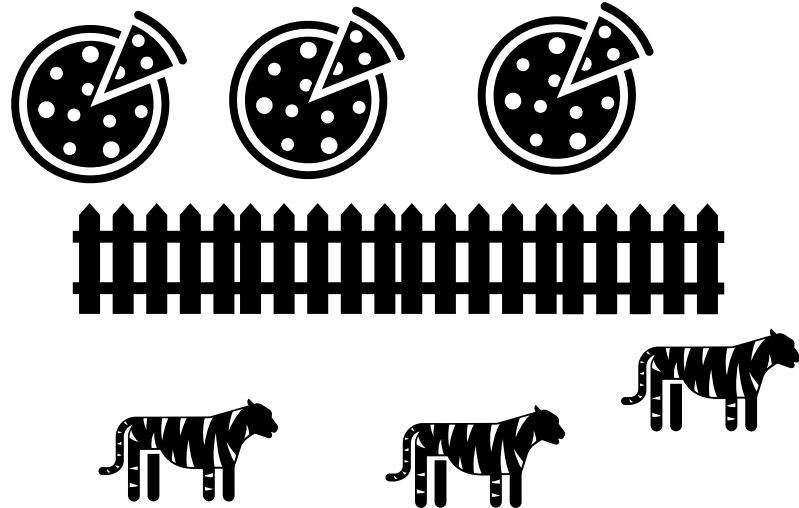


Firewalls

Definition:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

Pizzen sind vor den
Tigern sicher.



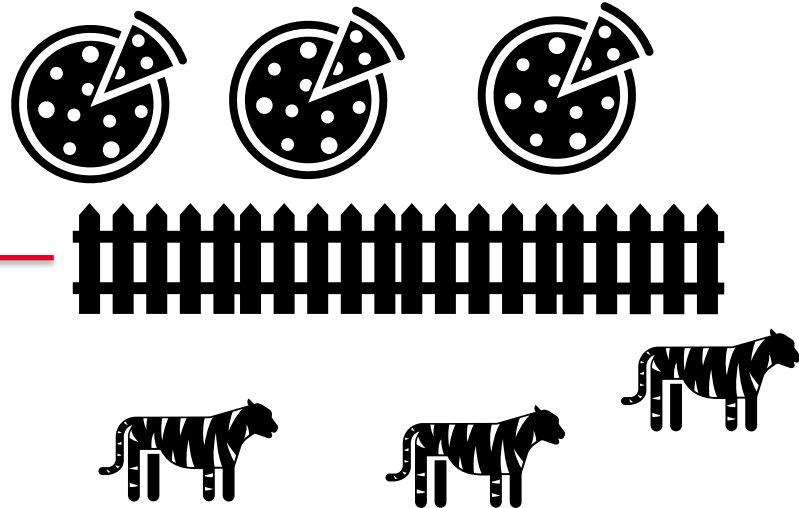
Firewalls

Definition:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

Pizzen sind vor den Tigern sicher.

Firewall



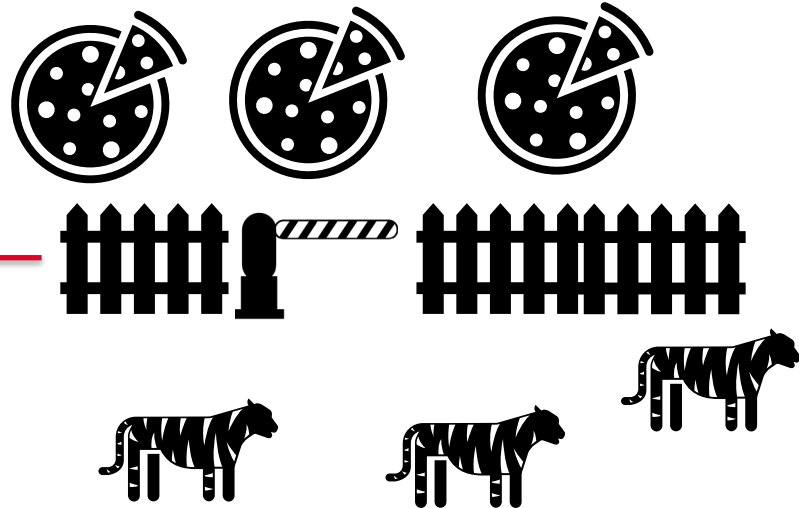
Firewalls

Definition:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

Pizzen sind vor den Tigern sicher.

Firewall



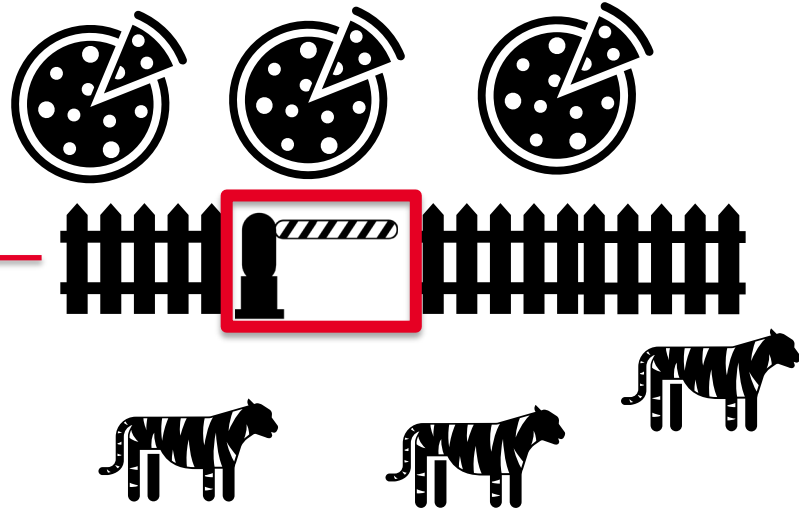
Firewalls

Definition:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

Pizzen sind vor den Tigern sicher.

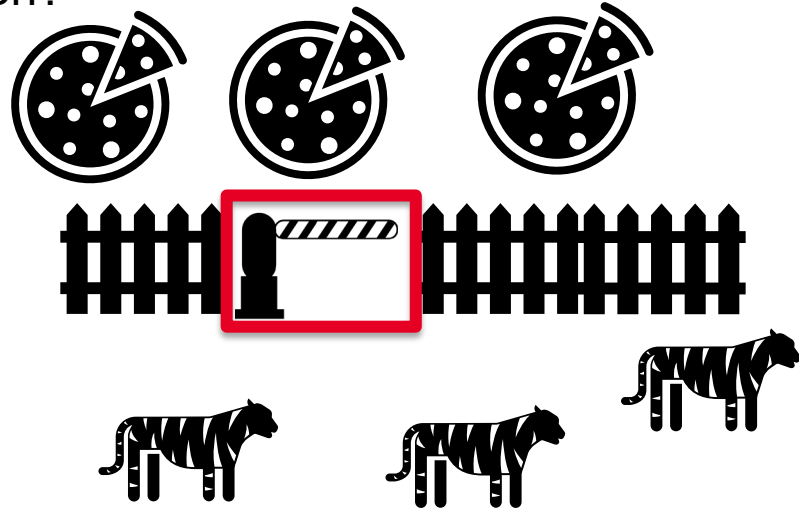
Firewall



Firewalls

Was wird an der Schranke geprüft?

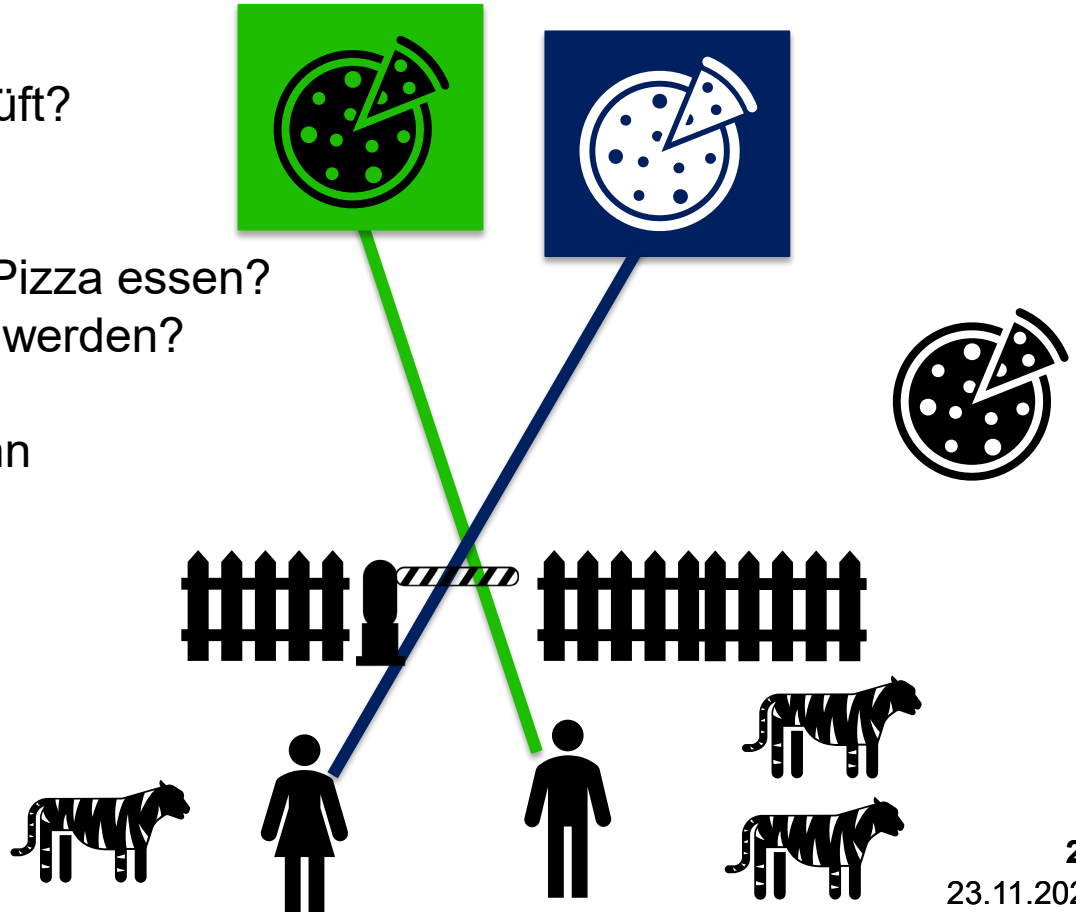
- Wer darf rein?
 - Wer darf etwas von der Pizza essen?
- Welche Pizza darf gegessen werden?
- Es wird festgehalten wer wann ein Stück gegessen hat.



Firewalls

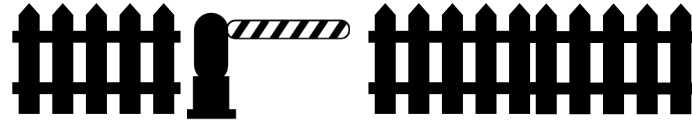
Was wird an der Schranke geprüft?

- Wer darf rein?
 - Wer darf etwas von der Pizza essen?
- Welche Pizza darf gegessen werden?
- Es wird festgehalten wer wann ein Stück gegessen hat.



Firewalls

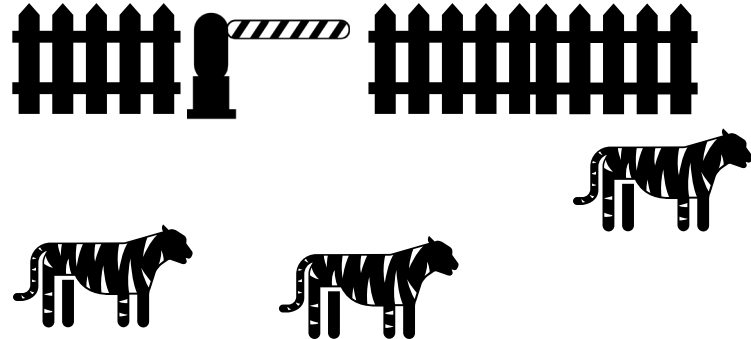
Andere Fragen die wichtig sind?



Firewalls

Andere Fragen die wichtig sind?

- Wer kam mit Hunger?
 - Wer hat viel Pizzastücke gekostet?



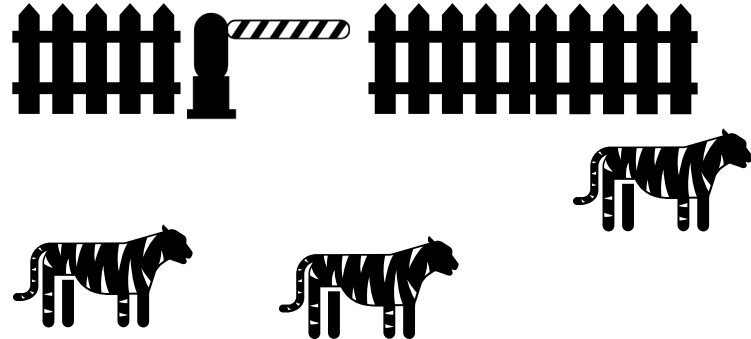
Firewalls

Andere Fragen die wichtig sind?

- Wer kam mit Hunger?
 - Wer hat viel Pizzastücke gekostet?



Welcher Dienst erzeugt
viel Traffic über die
Firewall?



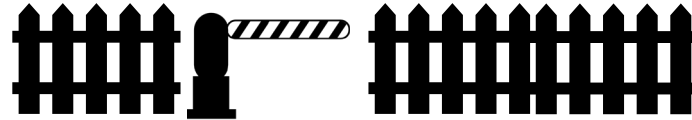
Firewalls

Andere Fragen die wichtig sind?

- Wer hat eine Pizza geklaut?



Wer hat unserem System Daten geklaut?



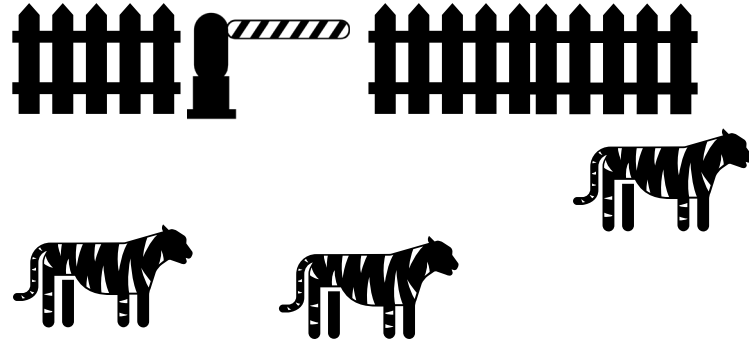
Firewalls

Andere Fragen die wichtig sind?

- Wer hat Thunfisch auf die Salamipizza getan?



Wer hat unsere Datenbank manipuliert?



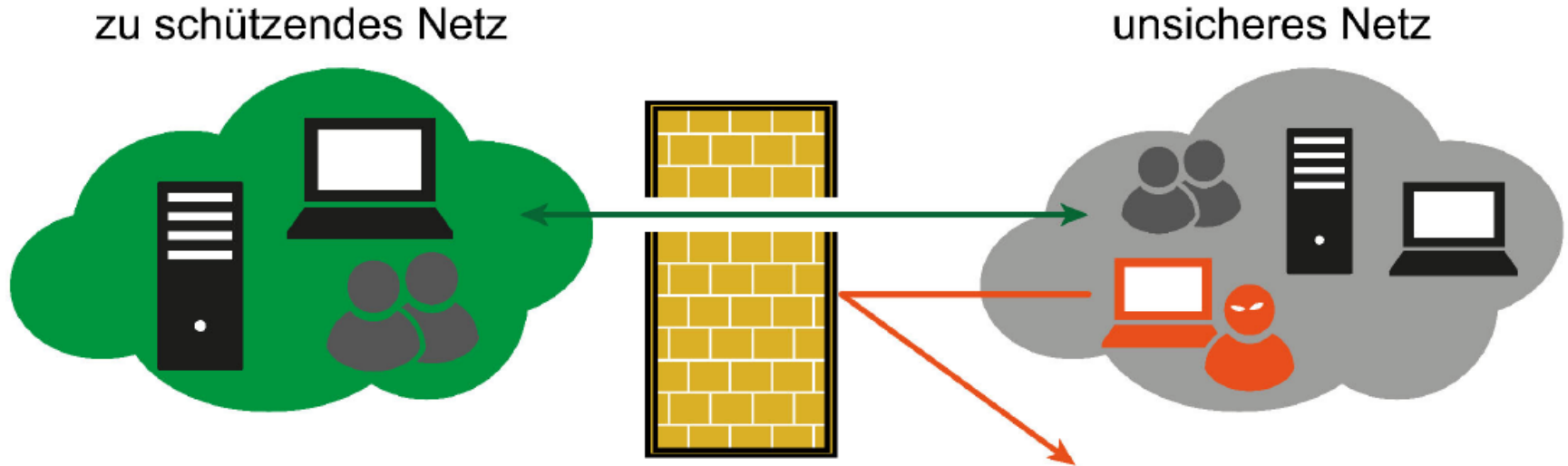
Firewalls

Zusammenfassung:

Ein **Firewall-System** ist dafür zuständig, einen **bestimmten IT-Bereich** meist in der **eigenen Organisation abzuschotten**, damit **Schäden**, die **außerhalb von diesem IT-Bereich auftreten**, nicht auf die **andere Seite übergreifen**.

- Wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf.
- Welche Protokolle und Dienste zugegriffen werden darf.
- Mit welchen IT-Systemen kommuniziert werden darf.

Firewalls



Firewalls

Detaillierte Aufgabenbereiche:



Firewalls

Beweissicherung und Protokollauswertung

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Zugangskontrolle auf Datenebene

Kontrolle auf der Anwendungsebene

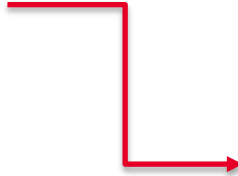
Rechteverwaltung

Vertraulichkeit der Nachrichten, wenn zusätzlich eine VPN-Funktion genutzt wird

Firewalls

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene



Kontrolle über
Vlans usw.

Firewalls

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Kopplung an das Active Directory




Firewalls

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Kopplung an
den Storage
Server



Zugangskontrolle auf Datenebene


Firewalls

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Kopplung an
den Storage
Server



Zugangskontrolle auf Datenebene

Rechteverwaltung

Firewalls

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Zugangskontrolle auf Datenebene

Rechteverwaltung



Firewalls

Detaillierte Aufgabenbereiche:


Zugangskontrolle auf der Netzwerkebene

Kopplung an das Active
Directory

Zugangskontrolle auf Nutzerebene

Zugangskontrolle auf Datenebene

Rechteverwaltung



Firewalls

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Zugangskontrolle auf Datenebene

Kontrolle auf der Anwendungsebene

Rechteverwaltung

Beweissicherung und Protokollauswertung



Logs und
Nachrichtendetails zu
Spam etc.

Firewalls

Beweissicherung und Protokollauswertung

Detaillierte Aufgabenbereiche:

Zugangskontrolle auf der Netzwerkebene

Zugangskontrolle auf Nutzerebene

Zugangskontrolle auf Datenebene

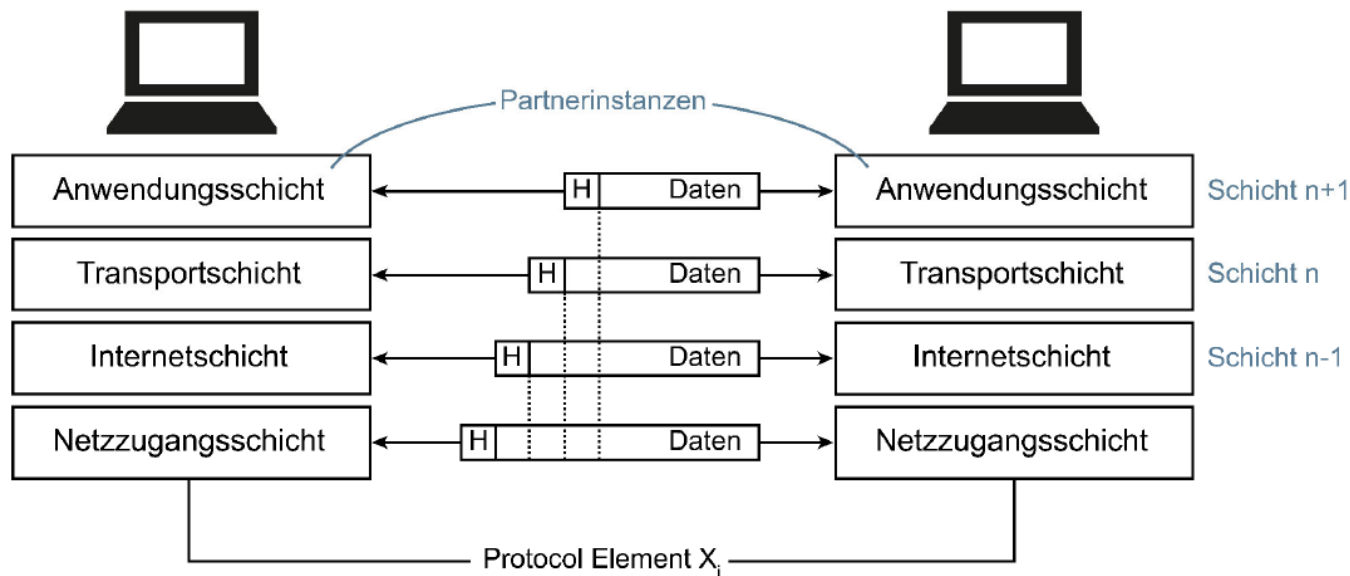
Kontrolle auf der Anwendungsebene

Rechteverwaltung

Vertraulichkeit der Nachrichten, wenn zusätzlich eine VPN-Funktion genutzt wird

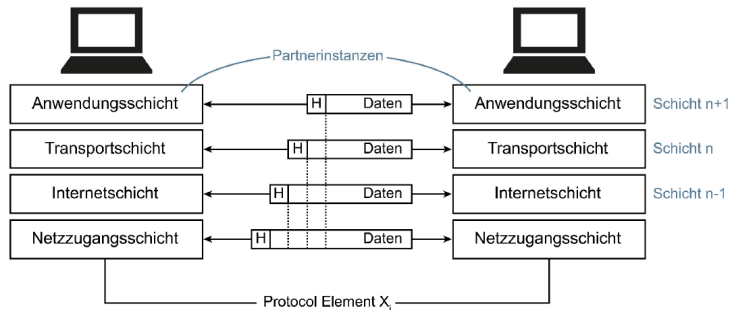
Firewalls

TCP-IP Protokollarchitektur:



Firewalls

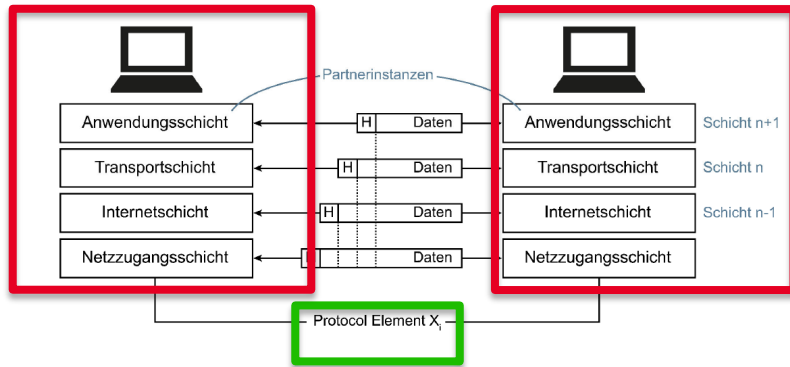
TCP-IP Protokollarchitektur:



- **N Instanzen** haben **Kontakt** zueinander
- Zwischen den **Instanzen** werden **Protokollelemente x_i** ausgetauscht

Firewalls

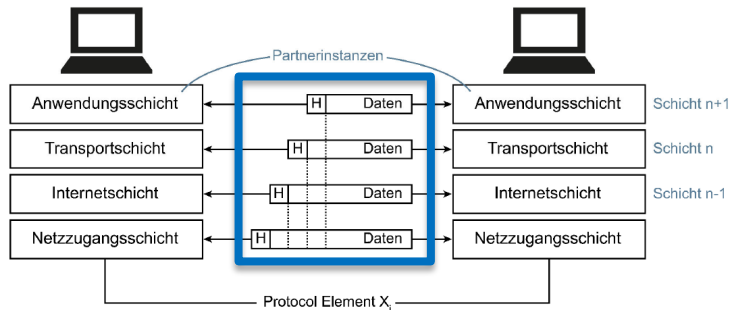
TCP-IP Protokollarchitektur:



- **N Instanzen** haben **Kontakt** zueinander
- Zwischen den **Instanzen** werden **Protokollelemente x_i** ausgetauscht

Firewalls

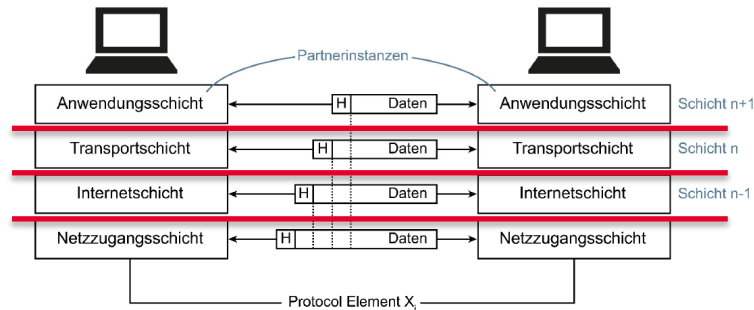
TCP-IP Protokollarchitektur:



- **N Instanzen** haben **Kontakt** zueinander
- Zwischen den **Instanzen** werden **Protokollelemente x_i** ausgetauscht
- **Header (H)** erhalten Setuerinformationen wie Adressen, laufende Nummern und Übertragungsweg

Firewalls

TCP-IP Protokollarchitektur:

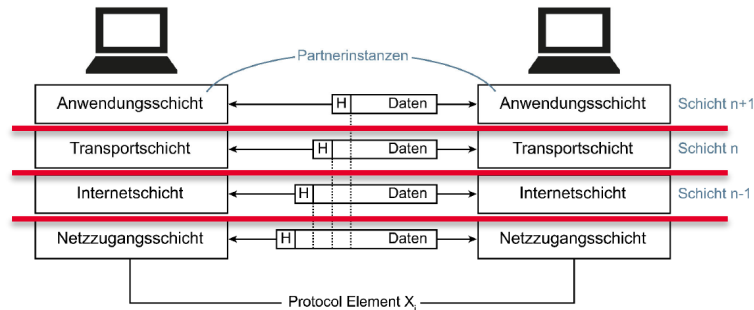


- **N Instanzen** haben **Kontakt** zueinander
- Zwischen den **Instanzen** werden **Protokollelemente x_i** ausgetauscht
- **Header (H)** erhalten Setuerinformationen wie Adressen, laufende Nummern und Übertragungsweg

Jede Schicht hat einen eigenen Header.

Firewalls

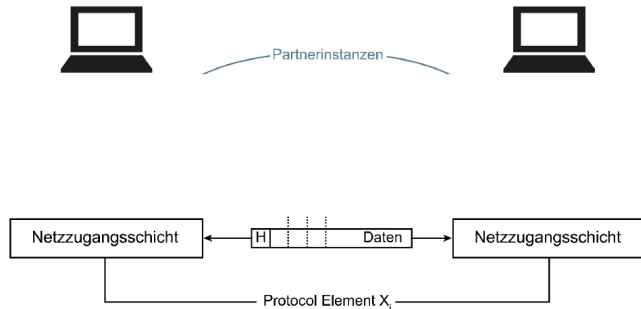
TCP-IP Protokollarchitektur:



- Daten werden von Schicht **N-1** nach **N** und dann nach **N+1** gegeben.
- Jede Schicht fügt Ihre Information an
- In welcher Reihenfolge wird im Kommunikationsprotokoll festgehalten
 - Hersteller Programmierung

Firewalls

TCP-IP Protokollarchitektur:

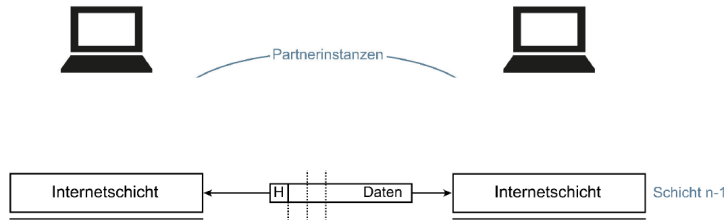


Netzzugangsschicht

- Ermöglicht die Datenübertragung über ein beliebiges Medium
- Verwendete Protokolle
 - Ethernet
 - WLAN
- Umfasst auch die Kapselung von IP-Paketen in Netzrahmen und die Zugriffssteuerung
 - Wer darf ins Netz?

Firewalls

TCP-IP Protokollarchitektur:

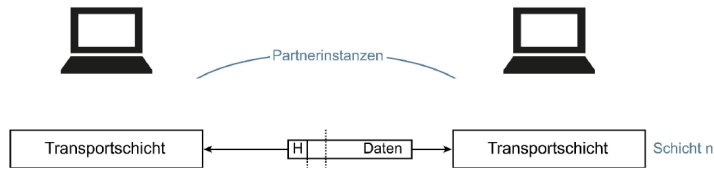


Internetschicht

- Definiert den Aufbau von IP Paketen und bestimmt welchen Weg diese nehmen (Routing)

Firewalls

TCP-IP Protokollarchitektur:

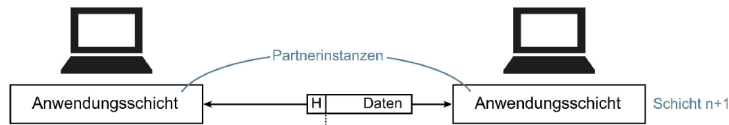


Transportschicht

- Stellt eine Verbindung zwischen zwei Endpunkten über das Netzwerk her
- Protokolle TCP und UDP
 - Halten fest das in **H** final steht

Firewalls

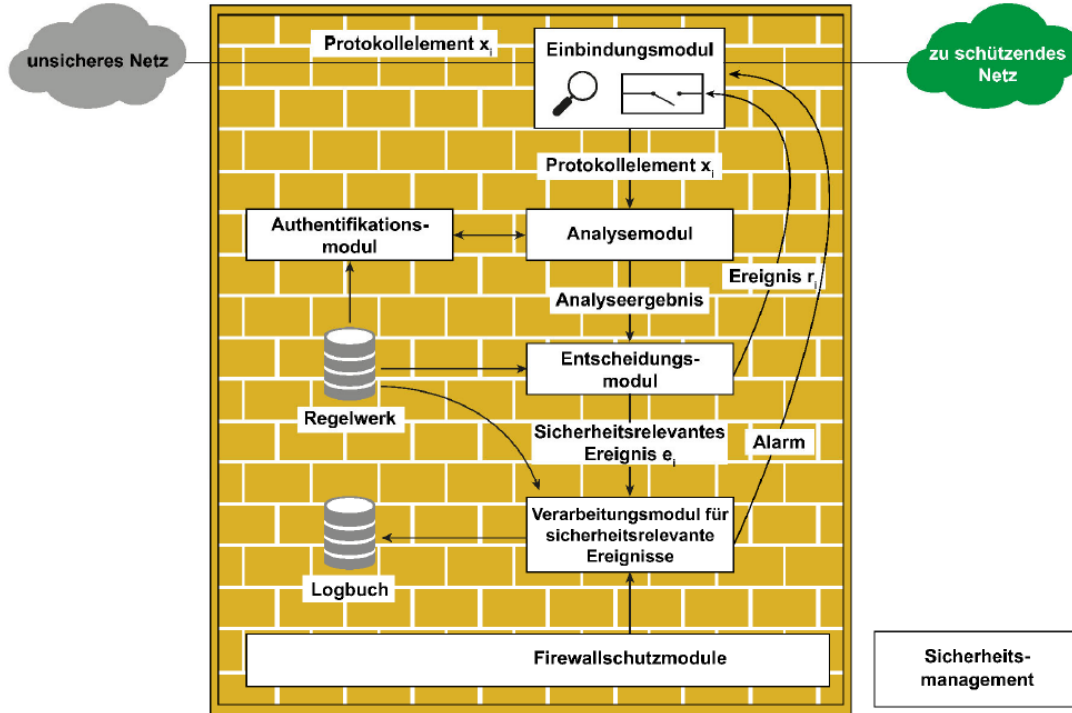
TCP-IP Protokollarchitektur:



Anwendungsschicht

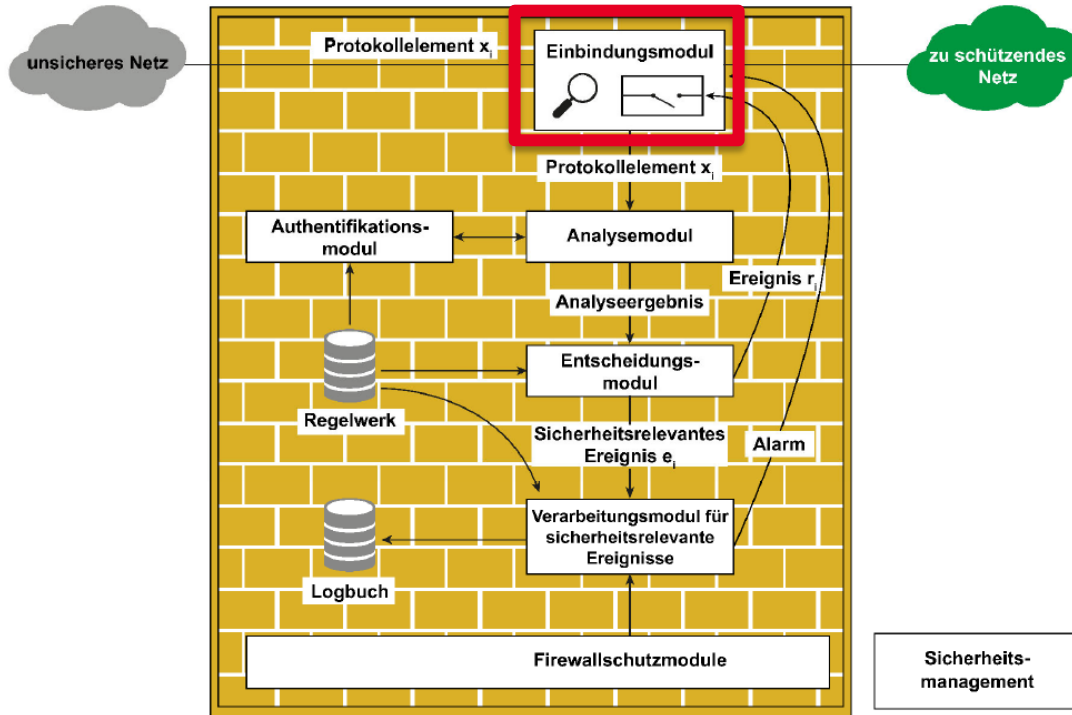
- Beinhaltet sämtliche Programme und Dienste die über Netzwerkzugang verfügen
- Protokolle wie HTTP, SMTP und FTP sind hier einzuordnen

Firewalls



Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

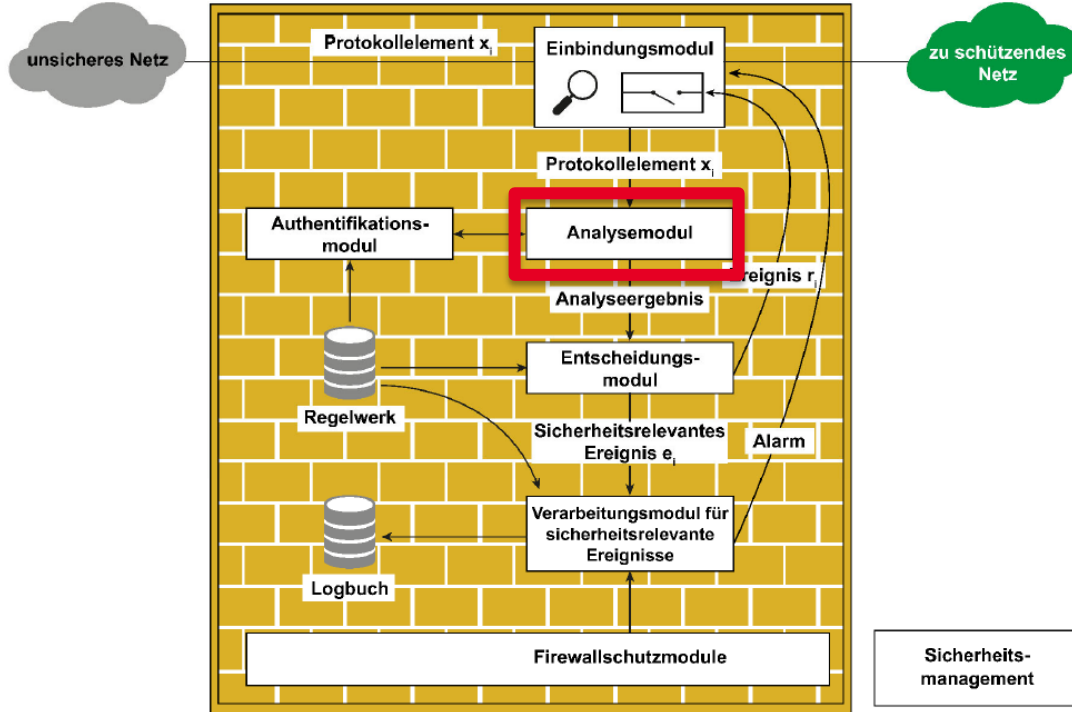
Firewalls



Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

Steht im Header etwas, was wir nicht erhalten wollen?

Firewalls



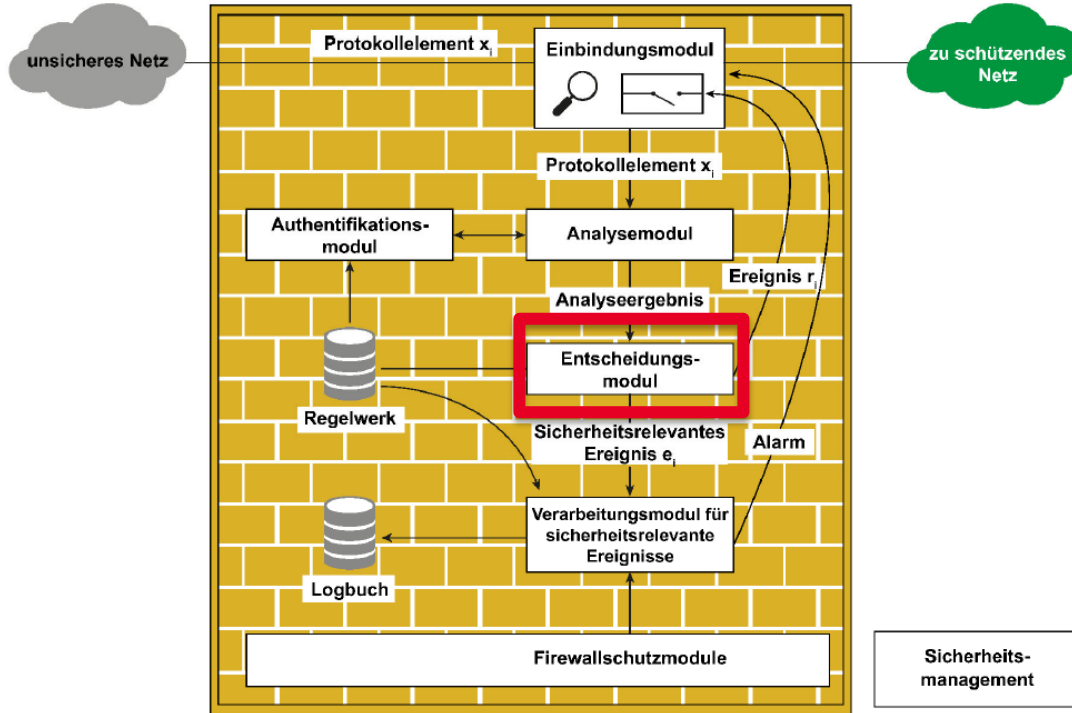
Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

Kompletter Datensatz wird analysiert.

Statusinformationen werden festgehalten.

Tiefer Scan entspricht langsamer performance.

Firewalls

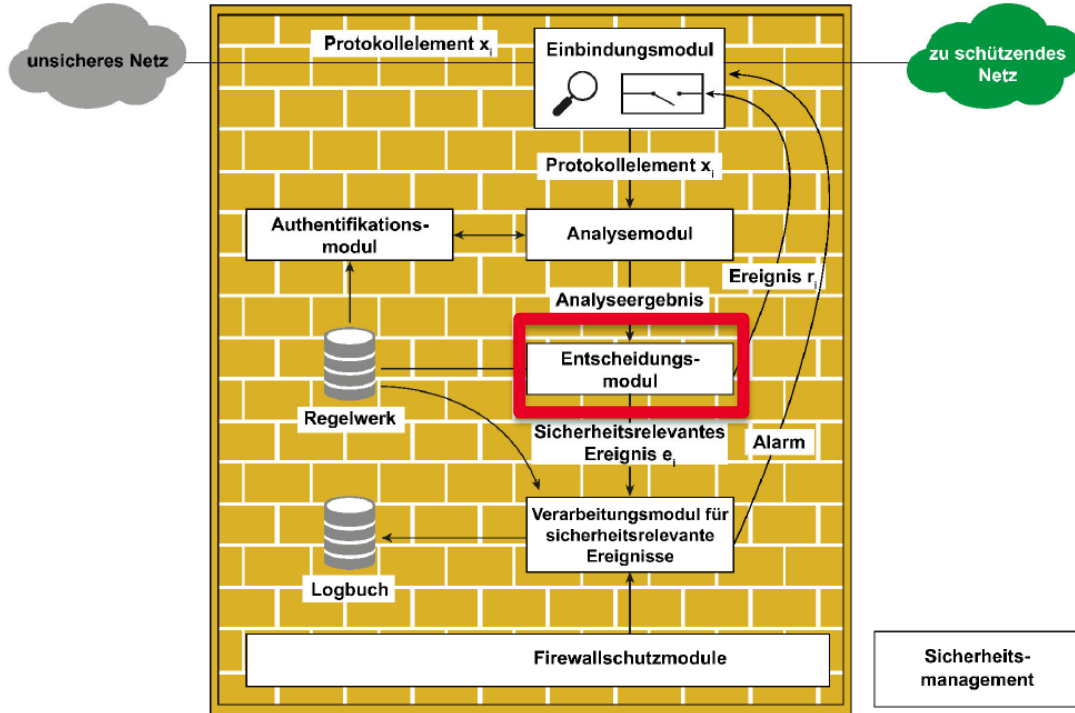


Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

Entscheidung wird getroffen in Abhängigkeit der Ergebnisse aus der Analyse.

result-of-decision (analysis ()), security-management ())

Firewalls



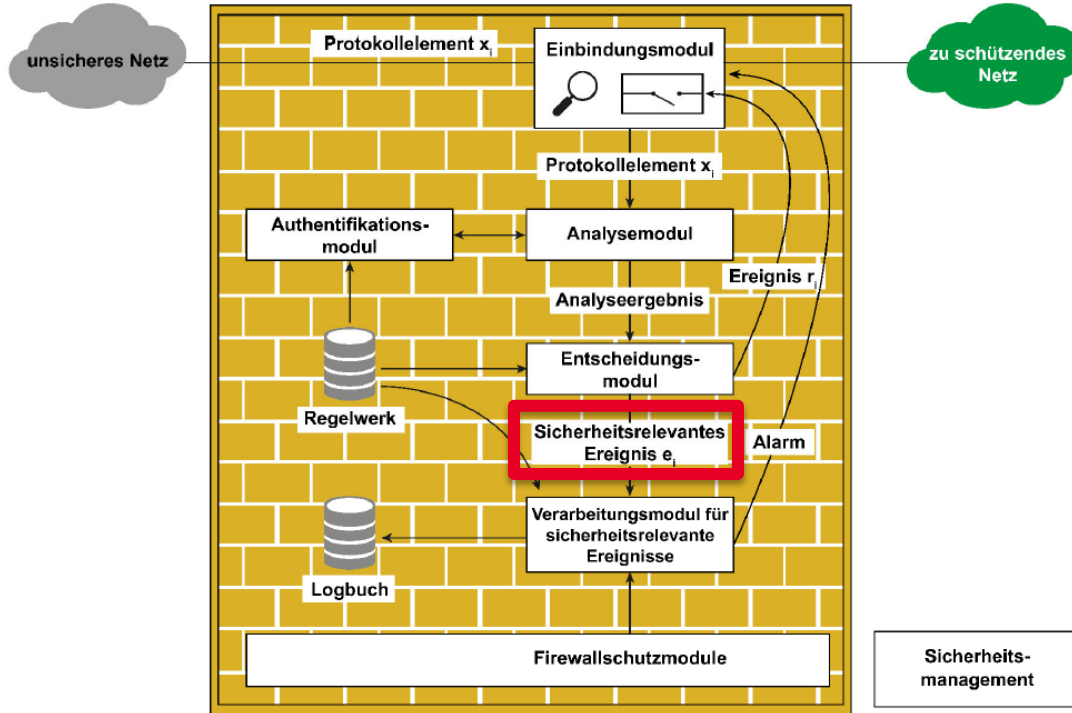
Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

Abgleich mit dem definierten Regelwerk.

Verbindung zu Sicherheitsrichtlinie.

result-of-decision (analysis ()), security-management ())

Firewalls

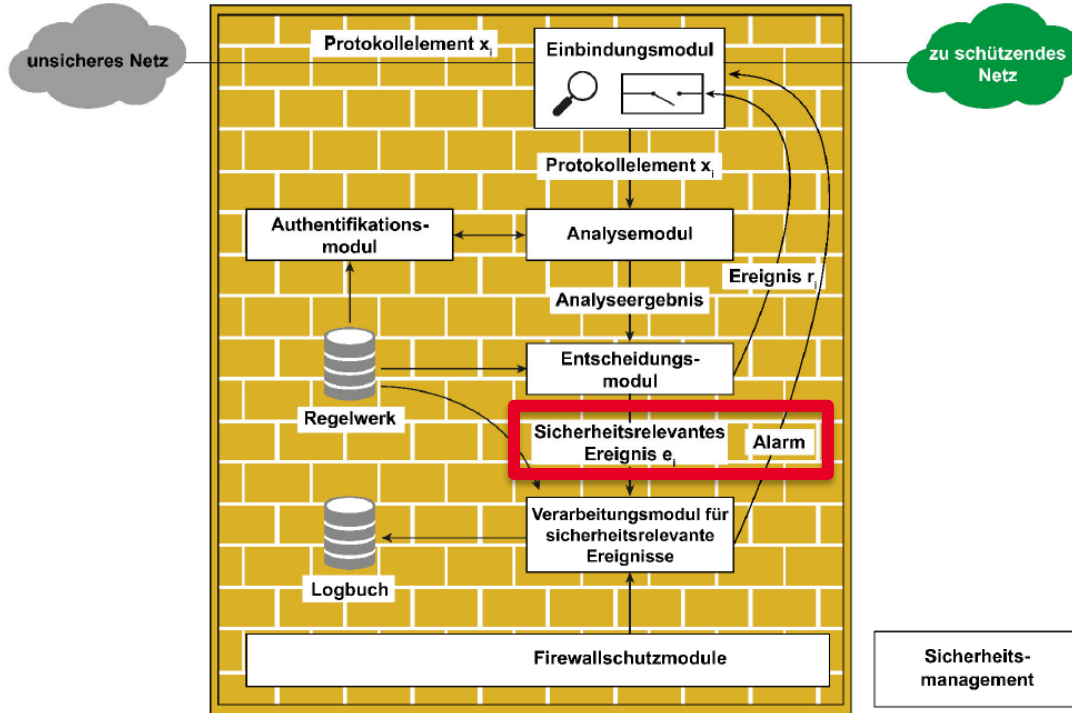


Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

event (e_i)

Das folgende Event kann ein Block von Spam sein.

Firewalls



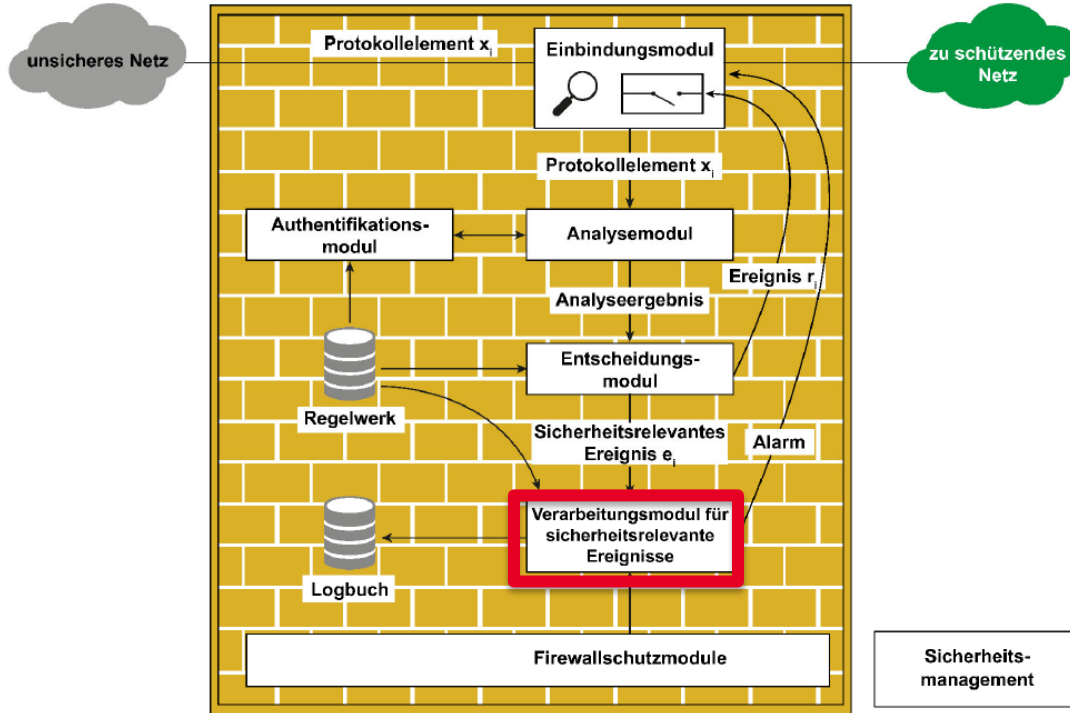
Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

event (e_i)

Block einer DDoS
Attacke.

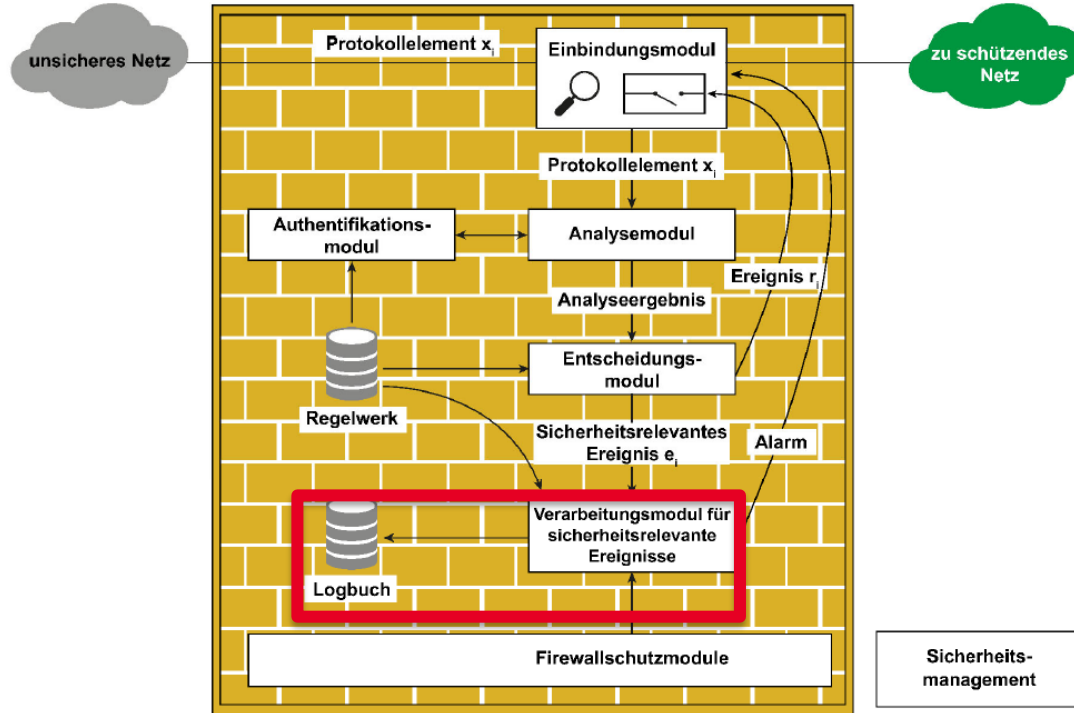
Alarm wird ausgelöst.

Firewalls



Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

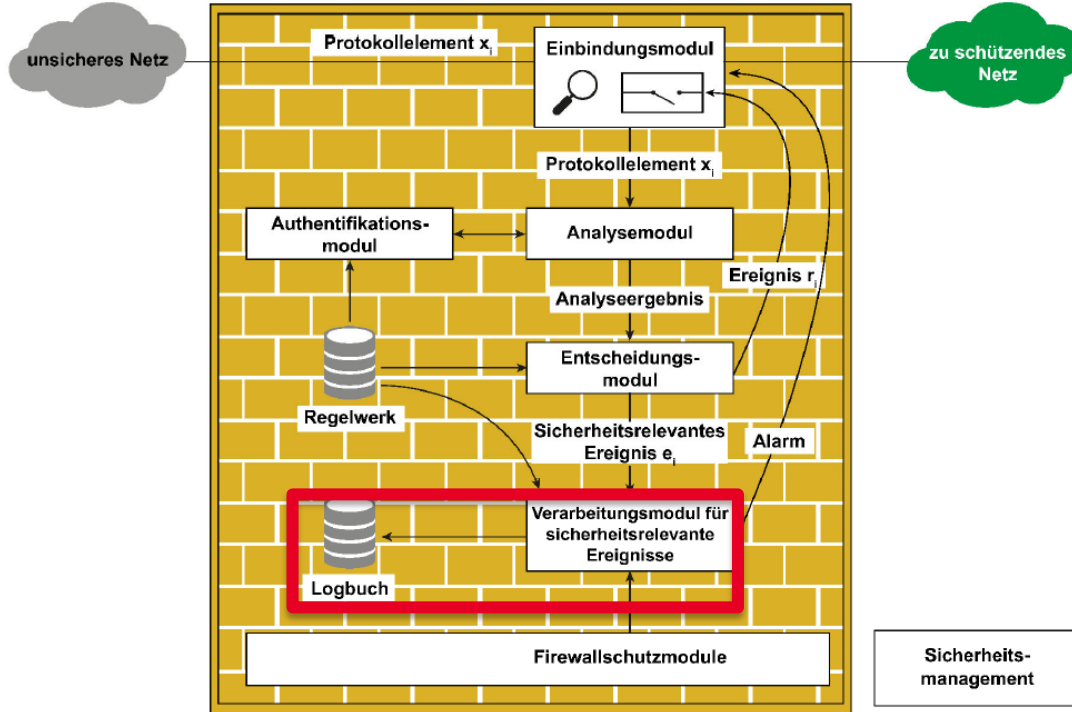
Firewalls



Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

Alle Entscheidungen werden in das Logbuch geschrieben.

Firewalls

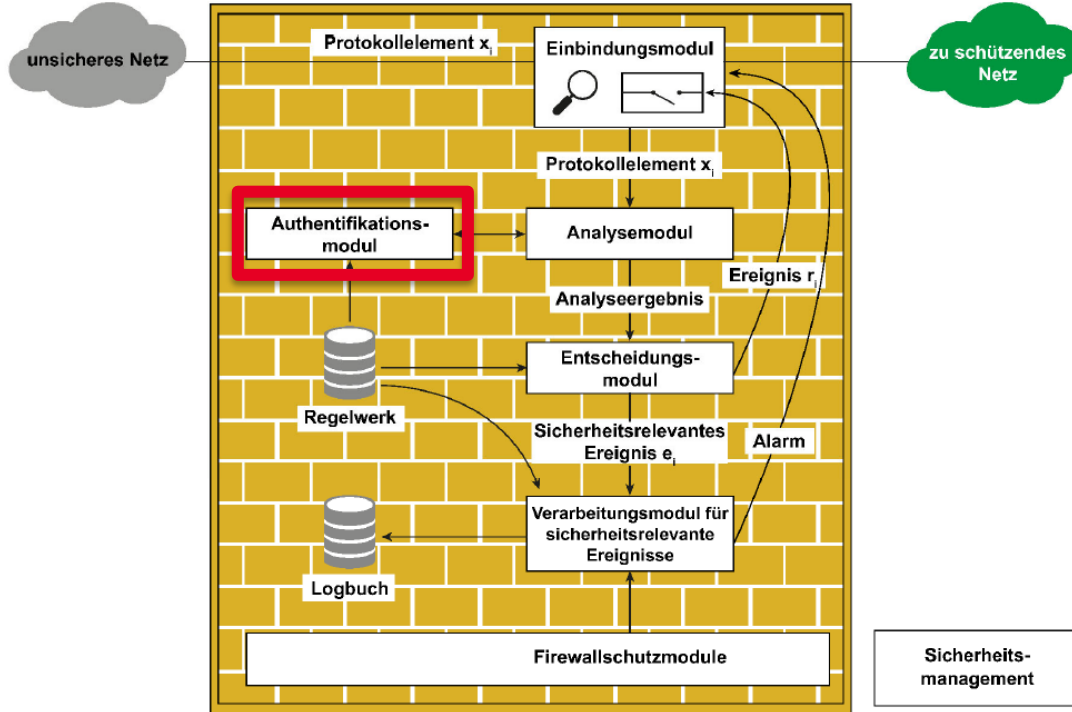


Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

Alle Entscheidungen werden in das Logbuch geschrieben.

Nachverfolgbar.

Firewalls



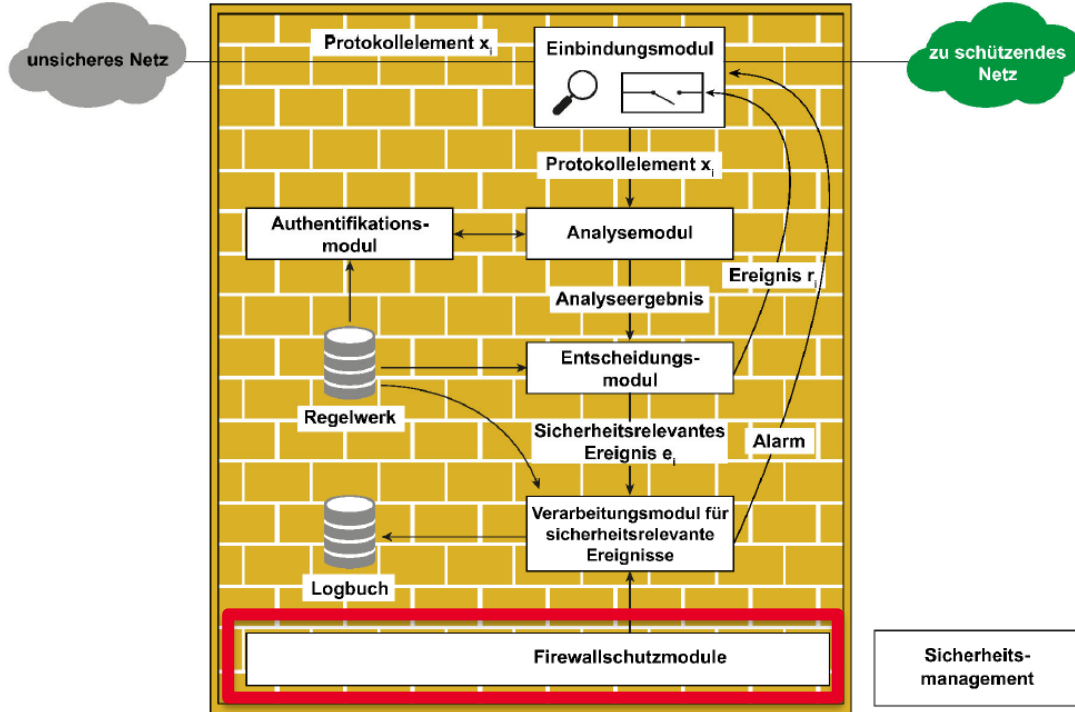
Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

authentication (t_i)

Sorgt für die Anmeldung an verwalteten Instanzen.

VPN User etc.

Firewalls



Protokollelement x_i läuft über das WWW in die Firewall und durchläuft verschiedene Module.

safeguard ()

Firewall Schutzmodul:

Bereich der programmierten Schutzfunktionen.

Hersteller Programmierung



Firewalls

Palo Alto Networks PA-5280 Firewall System bis 68 Gbps, 64 Mio Sessions, 2x AC Netzteil [PAN-PA-5280-AC]



228.318,24 € *

zzgl. 19% MwSt. i.H.v. 43.380,47 €

Bruttopreis: 271.698,71 €

versandkostenfreie Lieferung innerhalb Deutschlands ab 150 Euro

● Lagerbestand: 0 | Lieferzeit bis zu 60 Werktage

Kauf auf Rechnung / Firmenlastschrift? » Mehr Infos hier

1

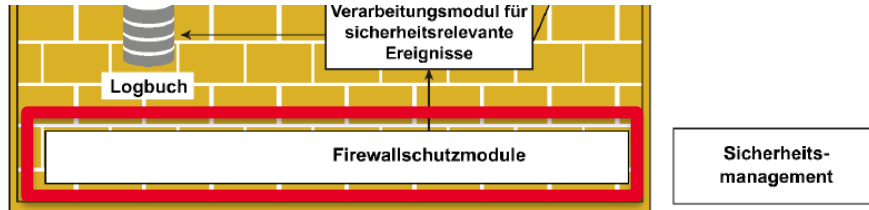
In den Warenkorb

■ Konfiguration speichern

♥ Merken

Artikel-Nr.:

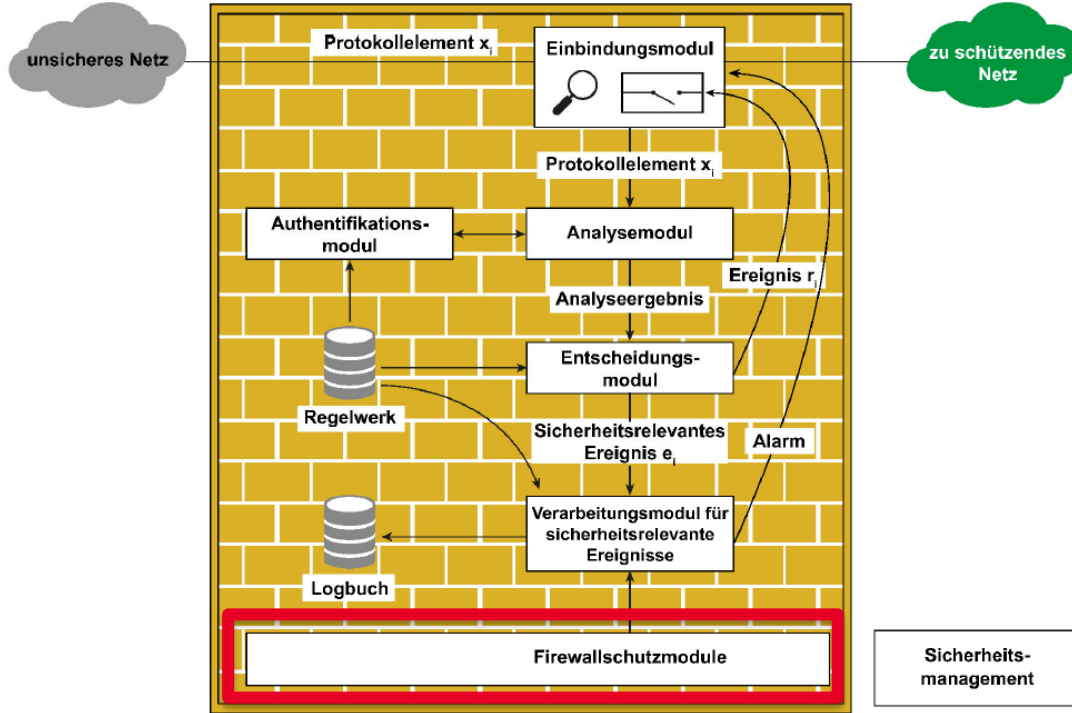
PAN-PA-5280-AC



Bereich der programmierten Schutzfunktionen.

Hersteller Programmierung

Firewalls



Integritätstest:

Ist die Firewall manipuliert worden?

TPM Check beim Bootvorgang.

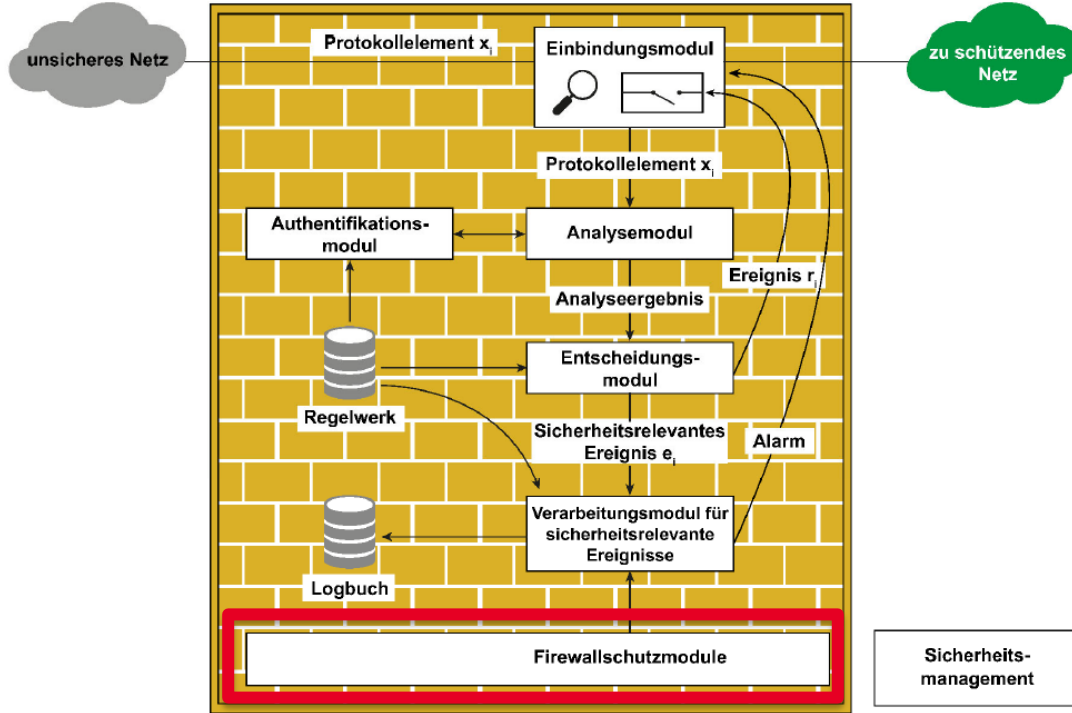
safeguard ()

Firewall Schutzmodul:

Bereich der programmierten Schutzfunktionen.

Hersteller Programmierung

Firewalls



Integritätstest:

Checksummenüberprüfung wird durchgeführt.

Prüfsumme wird aus Speicherobjekten errechnet.

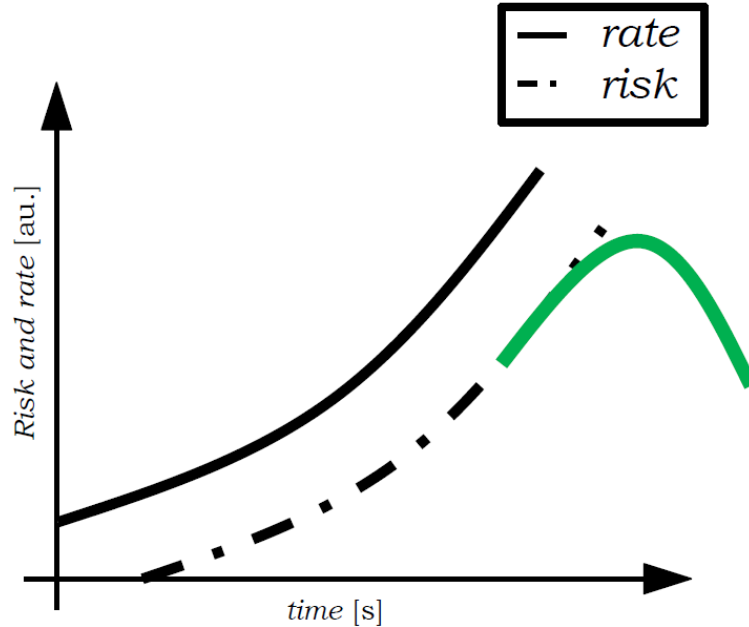
safeguard ()

Firewall Schutzmodul:

Bereich der programmierten Schutzfunktionen.

Hersteller Programmierung

Firewalls



safeguard ()

Firewall Schutzmodul:

Bereich der programmierten
Schutzfunktionen.

Hersteller Programmierung



Firewalls

Palo Alto Networks PA-5280 Firewall System bis 68 Gbps, 64 Mio Sessions, 2x AC Netzteil [PAN-PA-5280-AC]



228.318,24 € *

zzgl. 19% MwSt. (U.V. 43.380,47 €)

Bruttopreis: 271.698,71 €

versandkostenfreie Lieferung innerhalb Deutschlands ab 150 Euro

• Lagerbestand: 0 | Lieferzeit bis zu 60 Werktage

Kauf auf Rechnung / Firmenlastschrift? » Mehr Infos hier

1

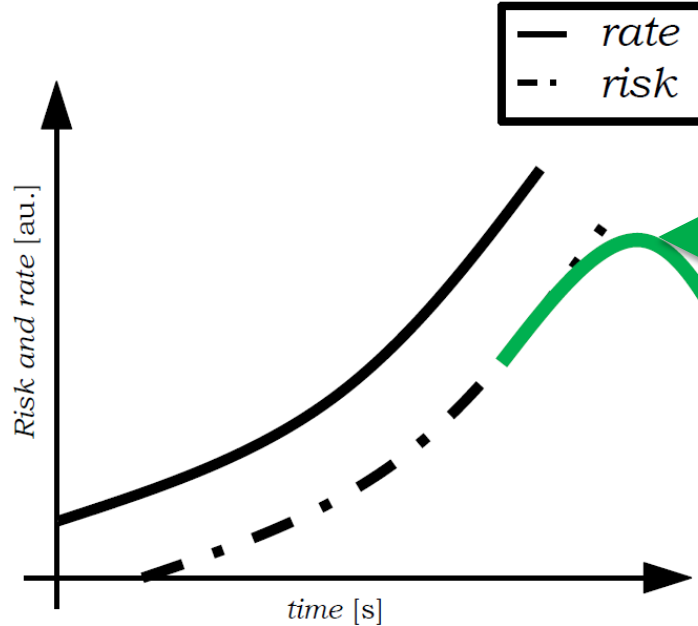
In den Warenkorb

Konfiguration speichern

Merken

Artikel-Nr.:

PAN-PA-5280-AC



Firewall Schutzmodul:

Bereich der programmierten
Schutzfunktionen.

Hersteller Programmierung



Firewalls

Palo Alto Networks PA-5280 Firewall System bis 68 Gbps, 64 Mio Sessions, 2x AC Netzteil [PAN-PA-5280-AC]



228.318,24 € *

zzgl. 19% MwSt. i.H.v. 43.380,47 €

Bruttopreis: 271.698,71 €

versandkostenfreie Lieferung innerhalb Deutschlands ab 150 Euro

● Lagerbestand: 0 | Lieferzeit bis zu 60 Werktage

Kauf auf Rechnung / Firmenlastschrift? » Mehr Infos hier

1

In den Warenkorb

■ Konfiguration speichern

♥ Merken

Artikel-Nr.:

PAN-PA-5280-AC

