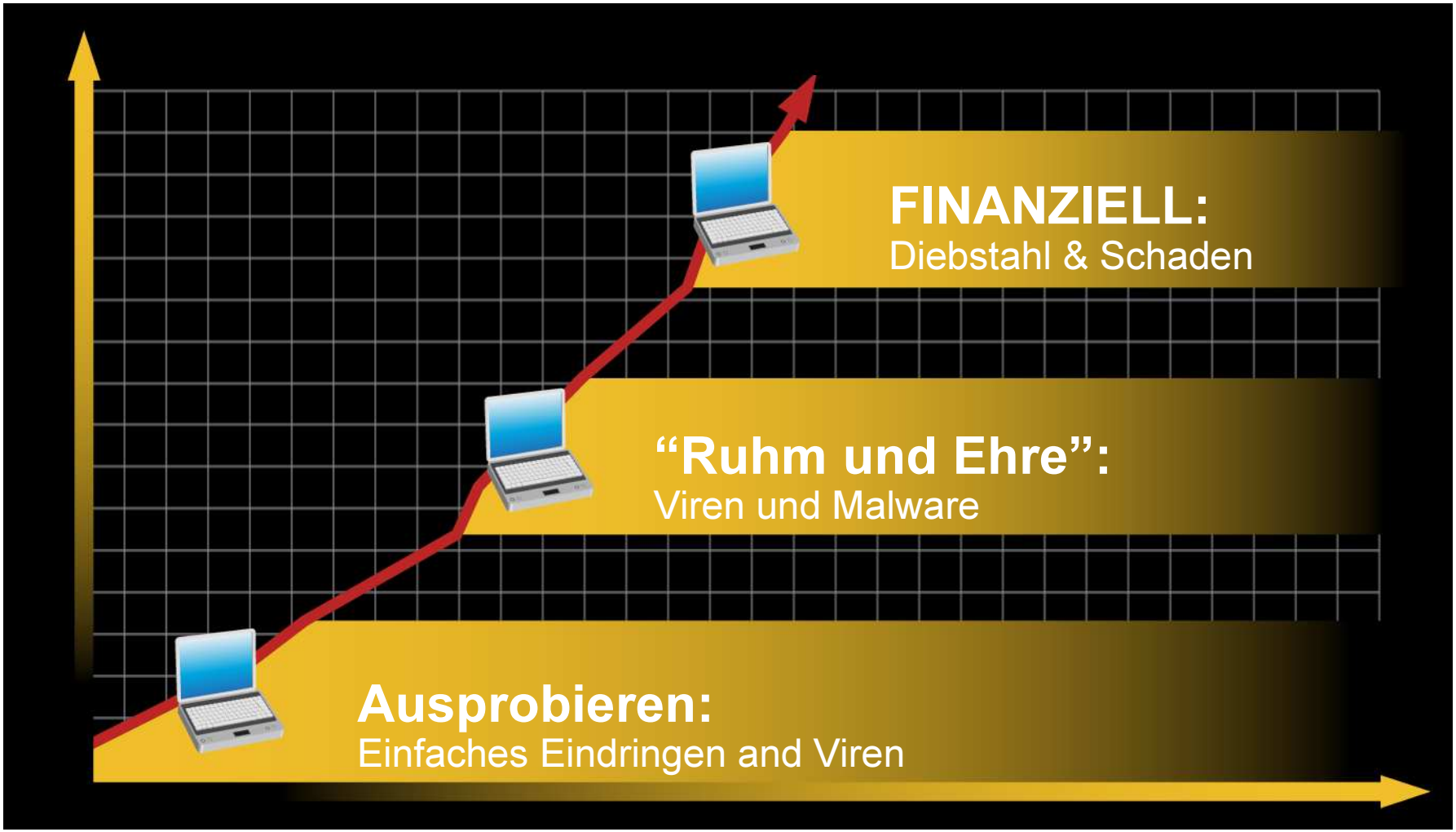
IT-Sicherheit

Stephan Meier
smeier@cisco.com

The Evolution der Ziele
Vom Hobbyisten zum Professional



Die Evolution der Bedrohungen

Breite Outbreaks

- Weit gefächert
- Belastung der IT
- Ärgerlich für User

Aber …

- Erfordert automatisierte Prozesse
- Mitwirken der User

Gezielte Angriffe

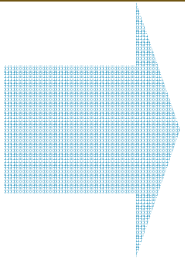
- Definiertes Ziel
- Business Verluste
- Vom User unbemerkt

Aber…

- Fast unsichtbar
- Geringes Wissen der User

Einfluss auf Produktivität — **Potentieller Schaden**

Anti-Virus
L3/L4 Firewall



Intrusion Prevention
Verhaltensanalyse
App. Gateway

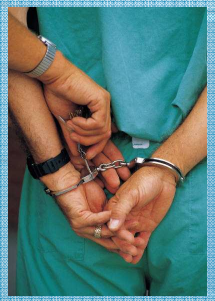
Einige Fakten:
Reale Bedrohungen beeinflussen reale Netze

James Ancheta,
Gelegenheits- Hacker aus Kalifornien

Ancheta benutzte verschiedenste Malware um die Kontrolle über weltweit **400,000** Computer zu übernehmen

Ancheta benutzte diese Machinen um **Hunderttausende** Dollar zu machen

- Vermieten der Machines an Spammer
- Installieren von Spyware auf den Machinen



Er wurde gefasst, als er Computer infizierte, die für die Waffenforschung der US Regierung genutzt wurden.

Im Mai 2006 zu 5 Jahren Gefängnis verurteilt

Spyware zum Verkauf
Die neue Firmen Spionage

- **Ruth und Michael Haephrati wird vorgeworfen, individuelle Spyware für Industriespionage zu erstellen**
- **Michael Haephrati hat 2000 angefangen Trojaner zu entwickeln**
- **Ehefrau Ruth Haephrati vermarktet diese 2004 an drei Private Ermittlungsunternehmen**
- **Die Spyware nutzt bekannte Sicherheitslücken in Windows Systemen**
- **Es wurden unter Nutzung von Standardverfahren diverse Daten gesammelt: Keystroke Logging, Screen Fapture, File Transfer, usw.**

"Organisierte Kriminelle sind sehr daran interessiert Informationen zu stehlen und Profit zu machen. Diese Tatsache signalisert sehr deutlich, daß die Gefahr durch Spyware zunimmt, und daß Firmen realiseren müssen, daß nicht nur Privatanwender betroffen sind."

Source: TechWeb
http://www.techweb.com/article/showArticle.jhtml;jsessionid=U45GMNUB4Y4VOQSNDLPSKH0CJUNN2JVN?articleId=181501294&pgno=2

Cisco Self-Defending Network:
Nutzung des Netzwerks um Bedrohungen zu Erkennen, zu Identifizieren und Einzudämmen

Integriert

Ermöglicht jedes Element im Netzwerk Punkt der Abwehr eines Angriffs oder einer Policy Umsetzung zu sein

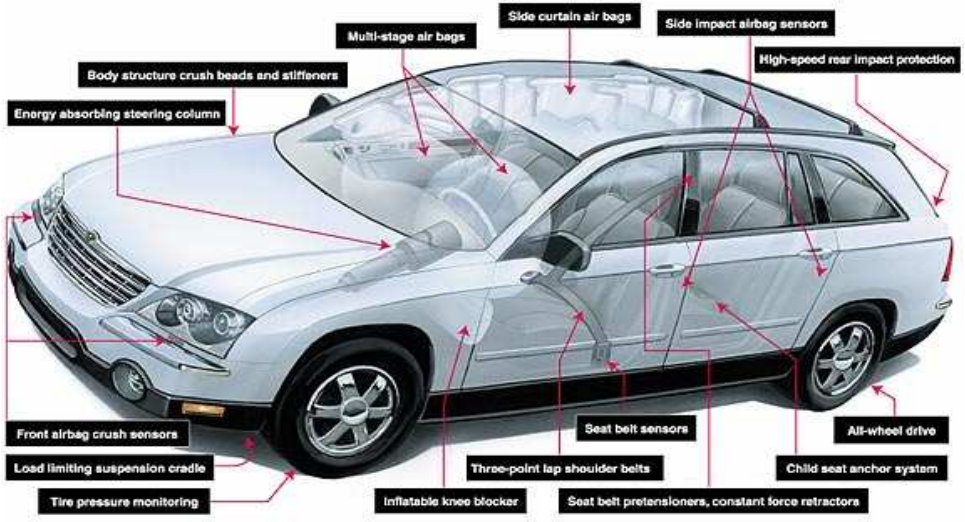
Zusammenwirkend

Zusammenwirken zwischen Funktionen und Geräten zur Abwehr eines Angriffs

Anpassungsfähig

Proaktive Security Technologien die Bedrohungen automatisch begegnen

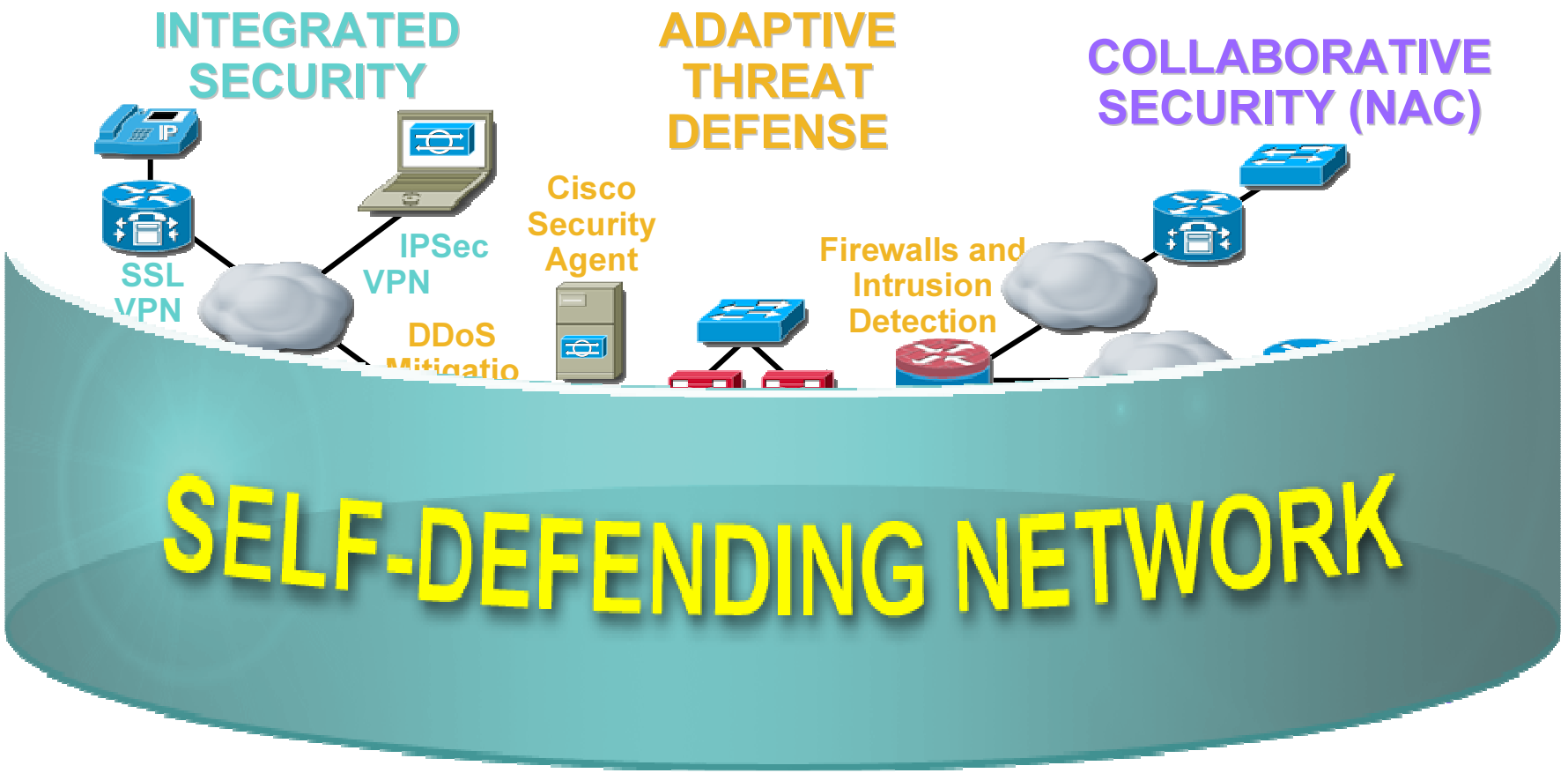
Vorteile eines Integrierten Ansatzes



- Komplexe Umgebung
- Lücken und Inkonstistent
- Geringer Überblick
- Schwierig zu managen
- Hohe TCO

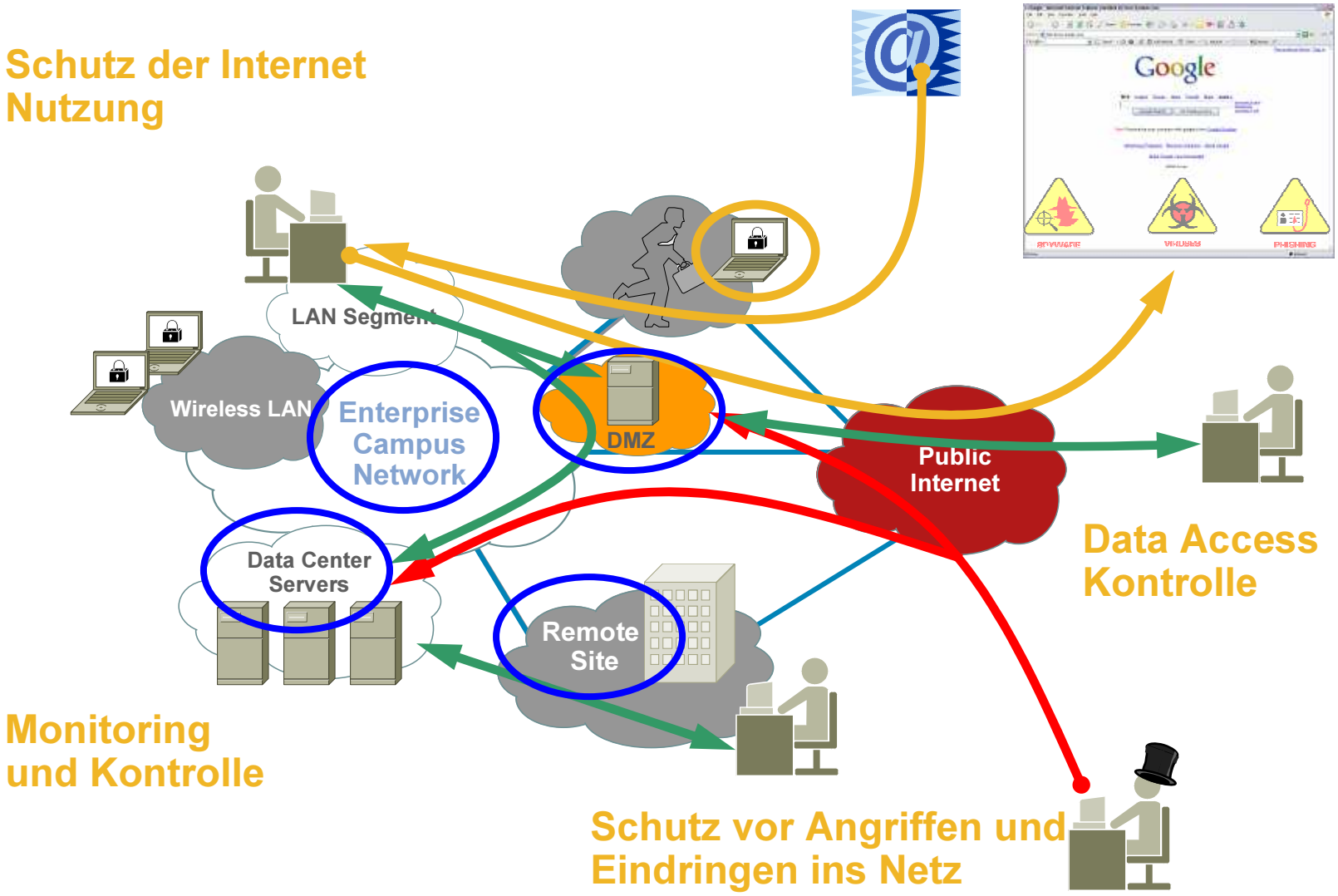
- Vereinfachte Umgebung
- Hohe Integration = hohe Sicherheit
- Hoher Überblick
- Einfach umzusetzen und zu managen
- Niedrige TCO

Self-Defending Network



Bestandteile des Self-Defending Networks

Lösungen zur Kontrolle und zum Eindämmen von Bedrohungen



Schutz der Internet Nutzung

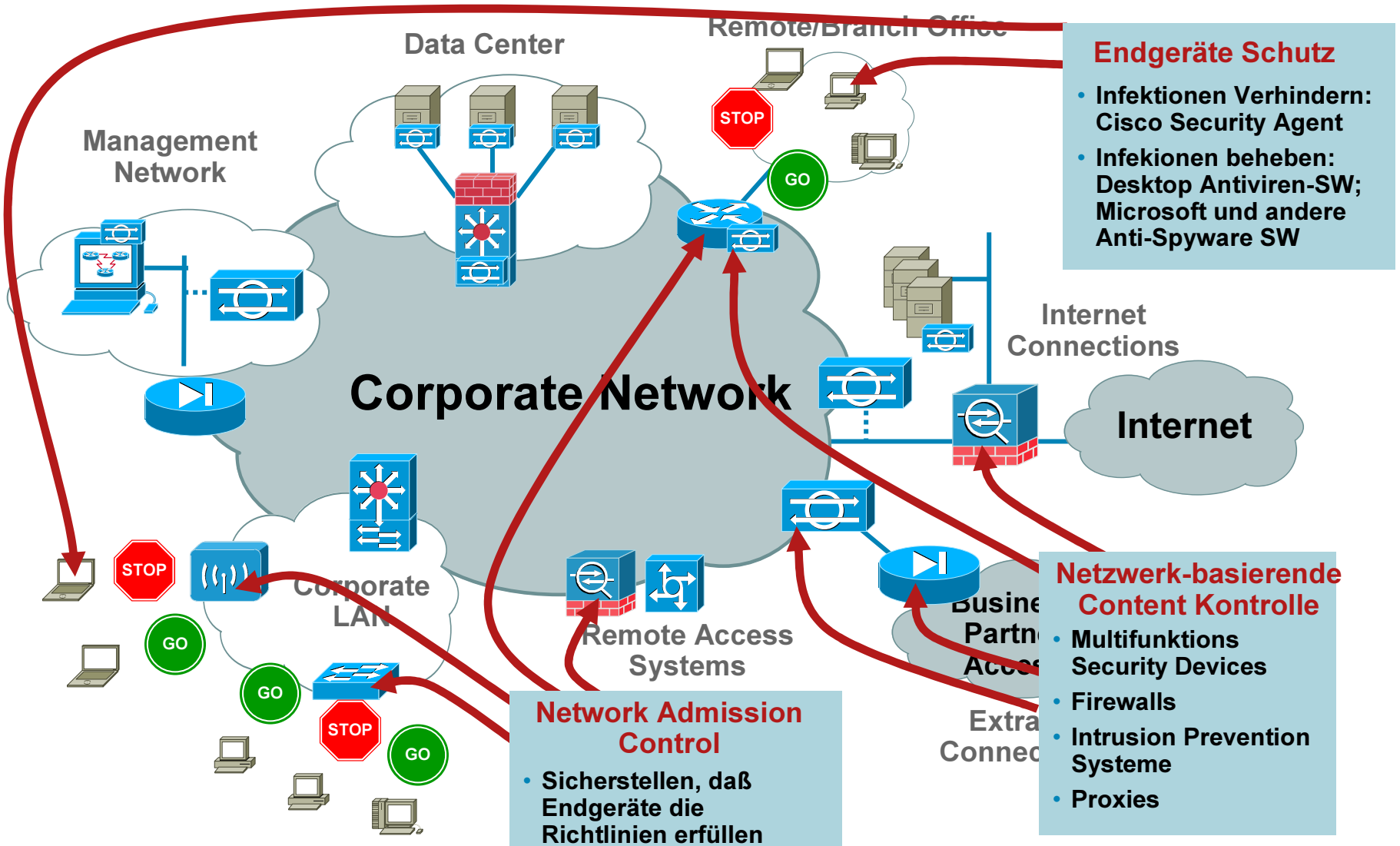
Intelligente Content Security
Cisco ASA mit CSC SSM: Kontrolliert neue Bedrohungen die sich über die normale Kommunikation einschleichen

Zugangsrichtlinien Kontrollieren
Cisco NAC: Verhindert das Einbringen von Bedrohungen durch den Netzwerkszugang mit infizierten Systemen

Endgeräte Schutz
CSA: Schützt interne Systeme vor den Folgen von Infektionen und deren Ausbreitung

Cisco ASA, Anti-X Technologien, CSA und NAC: Kontrollieren von Bedrohungen, Users schützen und Vertrauen schaffen

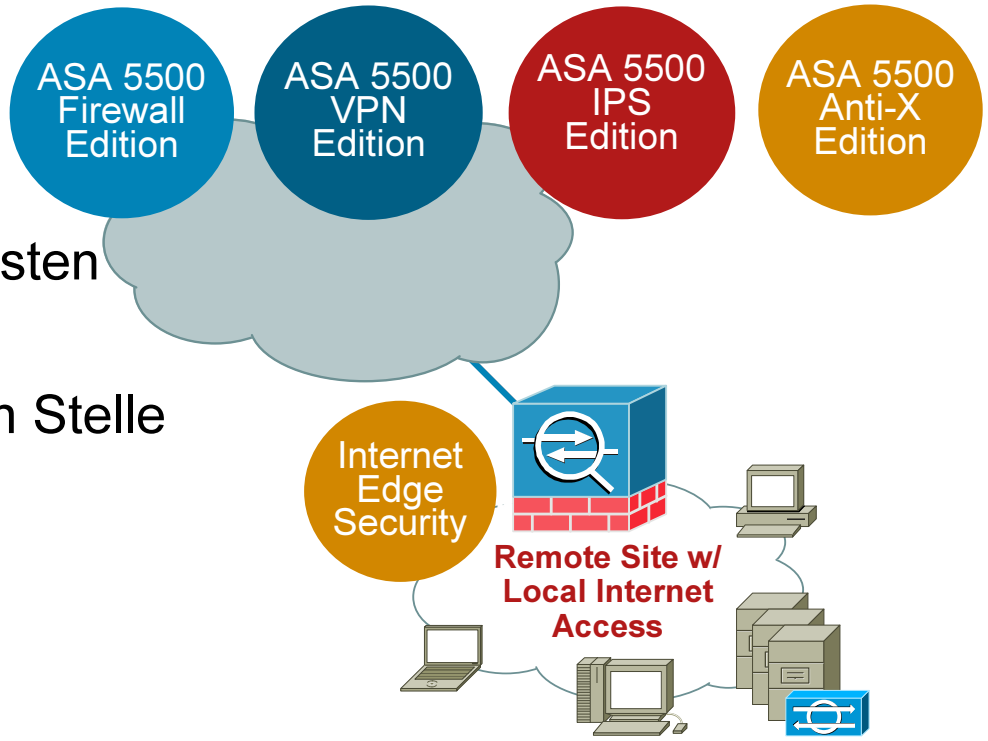
Kontrolle von Malware



Übergänge und Internet Zugänge mit der Cisco ASA 5500 Serie schützen

Schutz der Netzwerkzugänge erfordert eine leistungsfähige, integrierte Plattform

- Firewall und VPN Lösung der Enterprise Klasse
- Standardisierung minimiert Inbetriebnahme- und Betriebskosten
- Flexible Architekture liefert den richtigen Service an der richtigen Stelle
- Erweiterbar und Anpassbar



Cisco bietet die umfassendste Internet Gateway Security Lösung

Cisco ASA 5500 Serie Anti-X Edition

Bietet marktführende Content Security

Bedrohungsarten:

- Unerlaubter Zugang
- Eindringen und Angriffe
- Unsichere Verb.

Anti-X Service Erweiterung

- Viren
- Spyware
- Malware
- Phishing
- Spam
- Unerlaubte URLs
- Identity Theft
- Aggressive Inhalte

ASA 5500 mit CSC-SSM

Granulare Policy Kontrolle

Umfassender Malware Schutz

Fortschrittliche Content Filtererung

Integrierte Mail Security

Einfach zu Nutzen

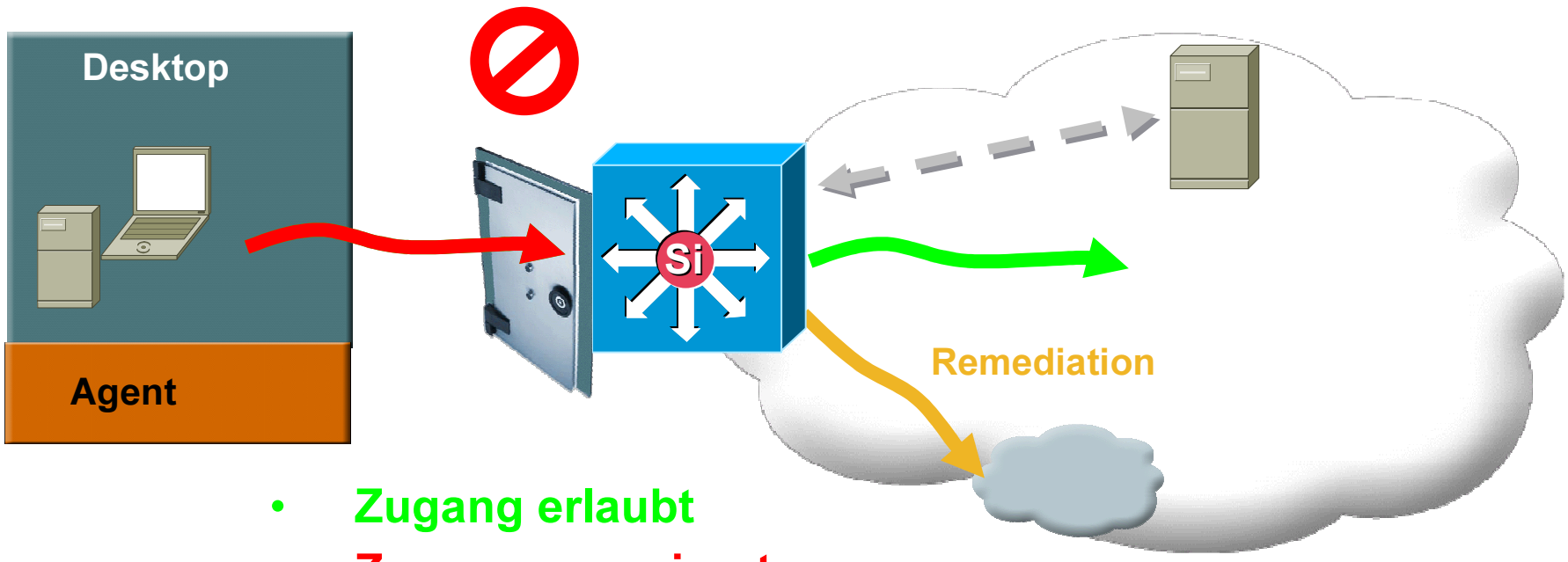
Technologie Partnerschaft

- Integrierte Trend Micro Antivirus und Content Security Technologien und Know How
- Bietet 24-Std Support gestützt durch führende Security Spezialisten

Network Admission Control in Aktion

Client baut Verbindung auf

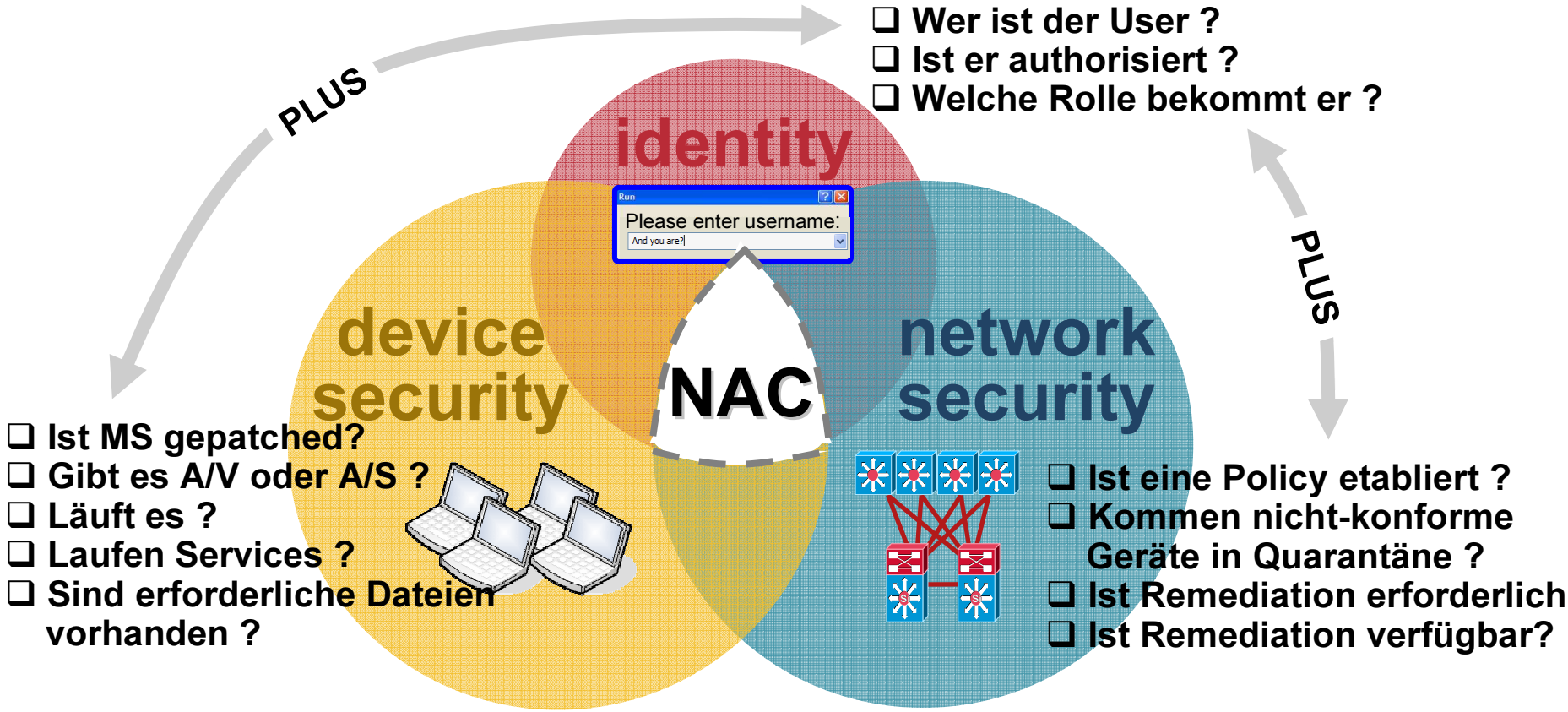
Authentifizierung und Überprüfung der Policy (Policy Server)



- Zugang erlaubt
- Zugang verweigert
- Quarantäne Remediation

Was ist Network Admission Control?

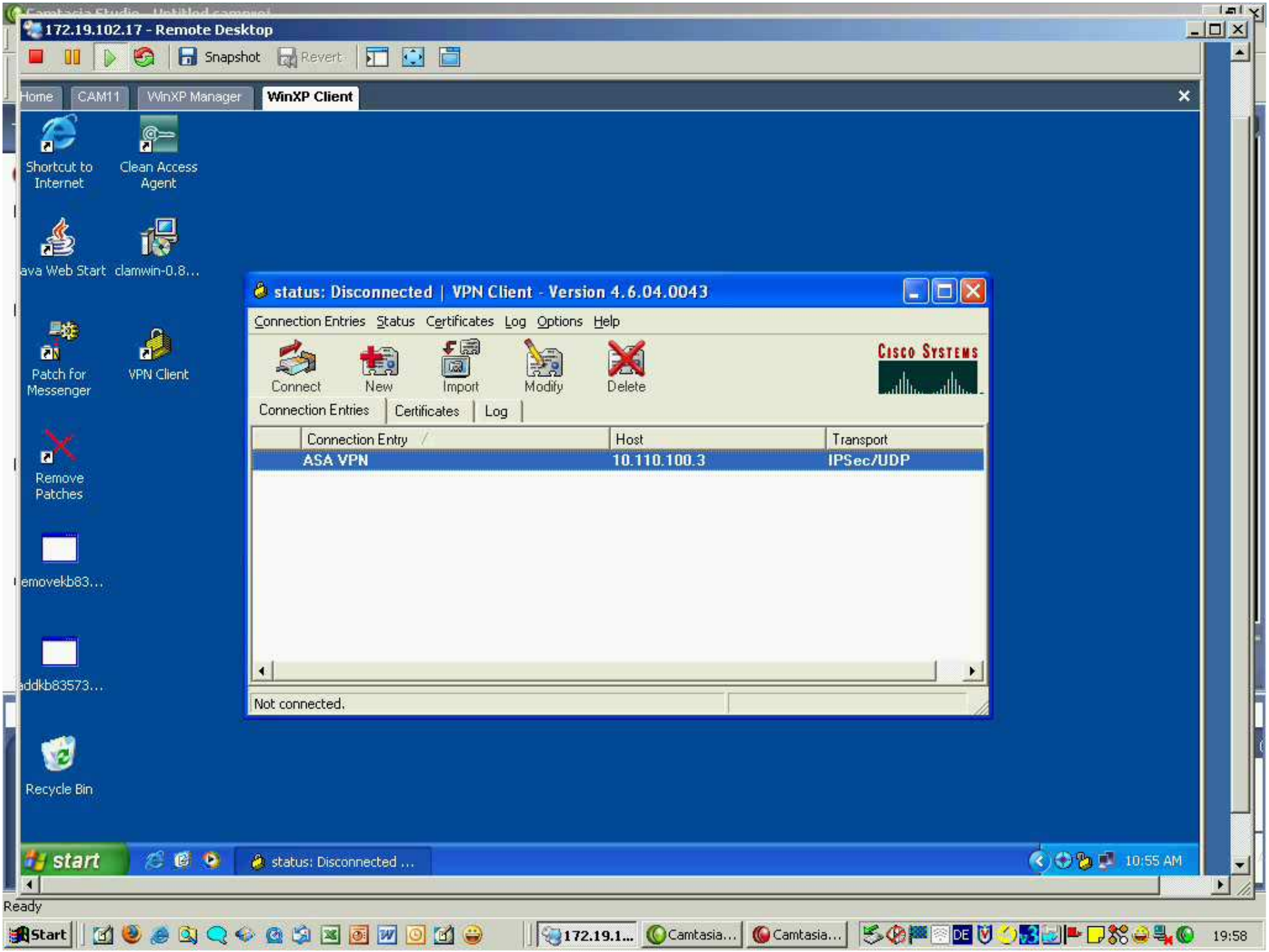
Nutzt das Netzwerk um zu erzwingen, daß reinkommende Endgeräte Regelkonform sind.



- ❑ Wer ist der User ?
- ❑ Ist er authorisiert ?
- ❑ Welche Rolle bekommt er ?

- ❑ Ist MS gepatched?
- ❑ Gibt es A/V oder A/S ?
- ❑ Läuft es ?
- ❑ Laufen Services ?
- ❑ Sind erforderliche Dateien vorhanden ?

- ❑ Ist eine Policy etabliert ?
- ❑ Kommen nicht-konforme Geräte in Quarantäne ?
- ❑ Ist Remediation erforderlich
- ❑ Ist Remediation verfügbar?


172.19.102.17 - Remote Desktop
Snapshot
Revert
Home
CAM11
WinXP Manager
WinXP Client
Shortcut to Internet
Clean Access Agent
ava Web Start
clamwin-0.8...
Patch for Messenger
VPN Client
Remove Patches
emovekb83...
addkb83573...
Recycle Bin
status: Disconnected | VPN Client - Version 4.6.04.0043
Connection Entries Status Certificates Log Options Help
Connect
New
Import
Modify
Delete
Cisco Systems
Connection Entries
Certificates
Log
Connection Entry
Host
Transport
ASA VPN
10.110.100.3
IPSec/UDP
Not connected.
start
status: Disconnected ...
10:55 AM
Ready
Start
172.19.1...
Camtasia...
Camtasia...
19:58

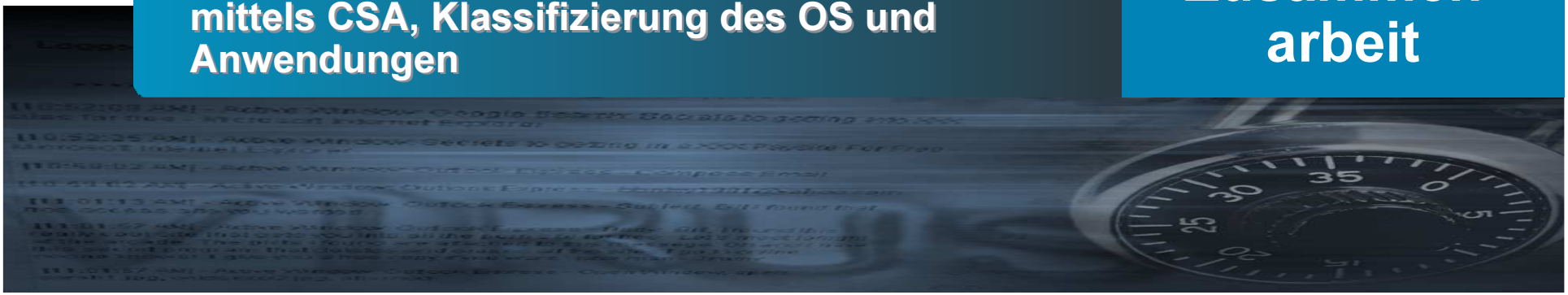
Schutz vor Angriffen und Eindringen ins Netz

Event Korrelation und Alarm Management
Korrelation und "eindampfen" von Events zur identifizierung von Bedrohungen mit CS-MARS

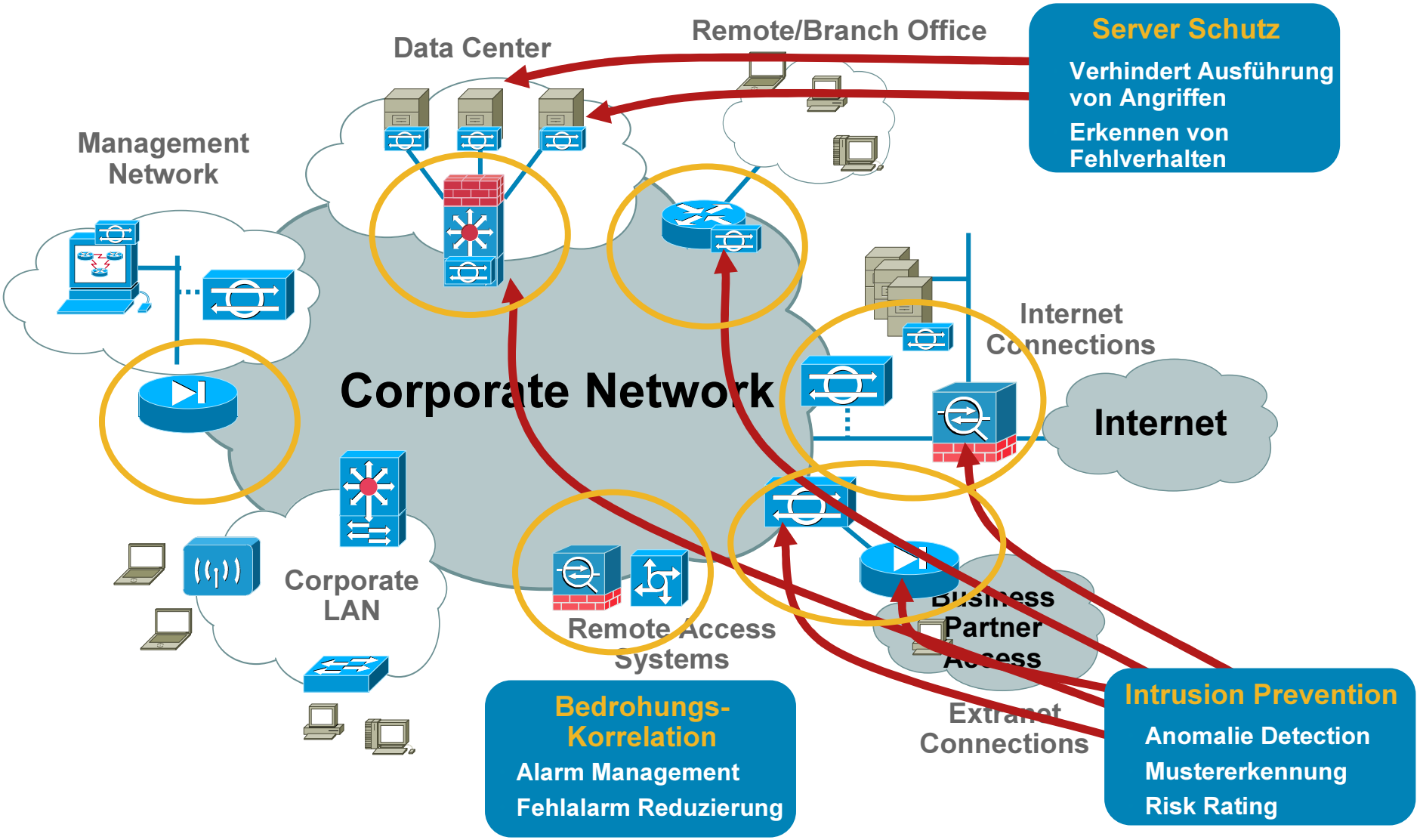
Identifizerung von Netzwerk Bedrohungen
Signature und Anomalie Erkennung und Analyse von Datenströmen mit IPS

Schutz der Endsysteme
Schutz vor Angriffen gegen Endsysteme mittels CSA, Klassifizierung des OS und Anwendungen

IPS, CSA, & CS-MARS identifizieren im Detail die Bedrohungen durch systemweite Zusammen-arbeit



Verhindert Angriffe und Eindringen

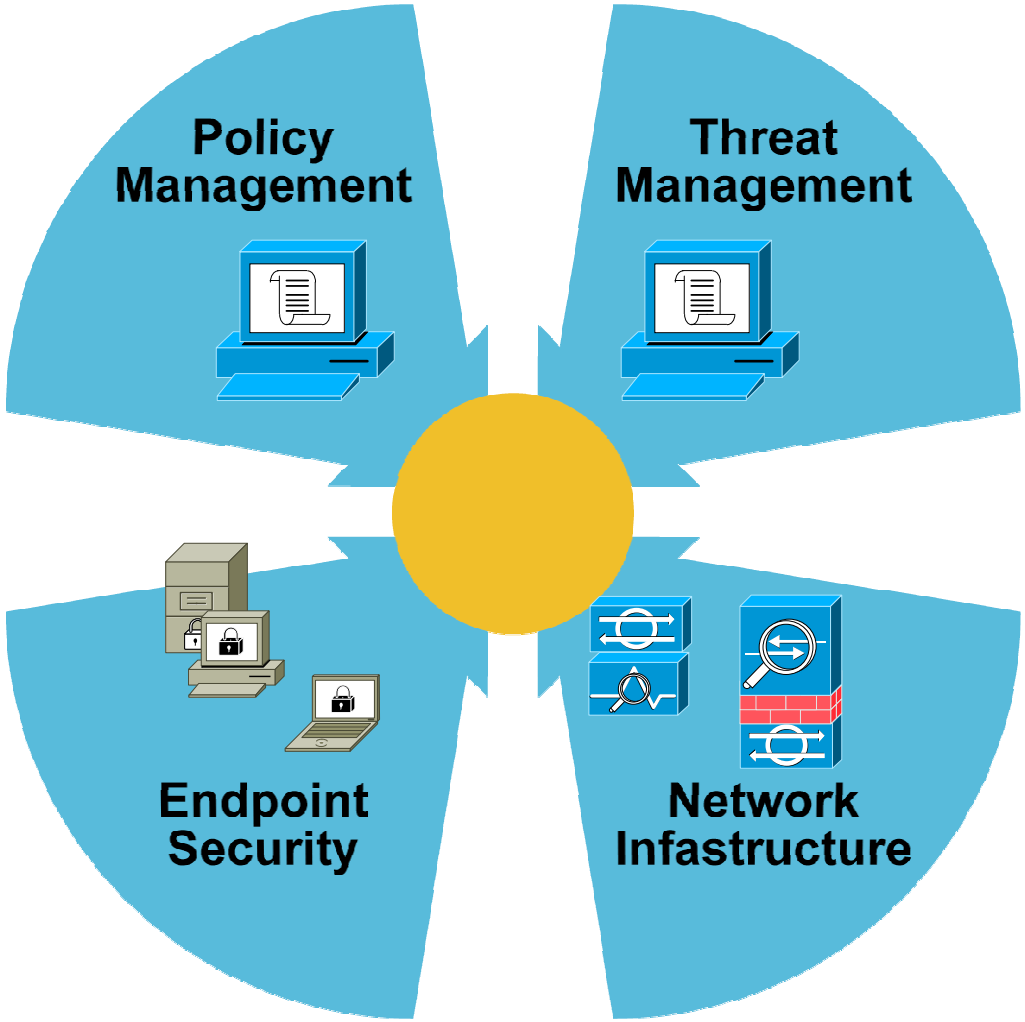


Zusammenarbeit der Systeme

Ermöglicht einfaches und wirksames Vorgehen

- **Verbessert Netzwerk-weite Sichtbarkeit**
- **Reduziert das Volumen der Information und Alarm**
- **Verbessert Relevanz der Information**
- **Verbessert Zuverlässigkeit der Signaturen**
- **Vermindert False Positives**

Beschleunigt die Erkennung und Abwehr von Bedrohungen, vereinfacht das Vorgehen

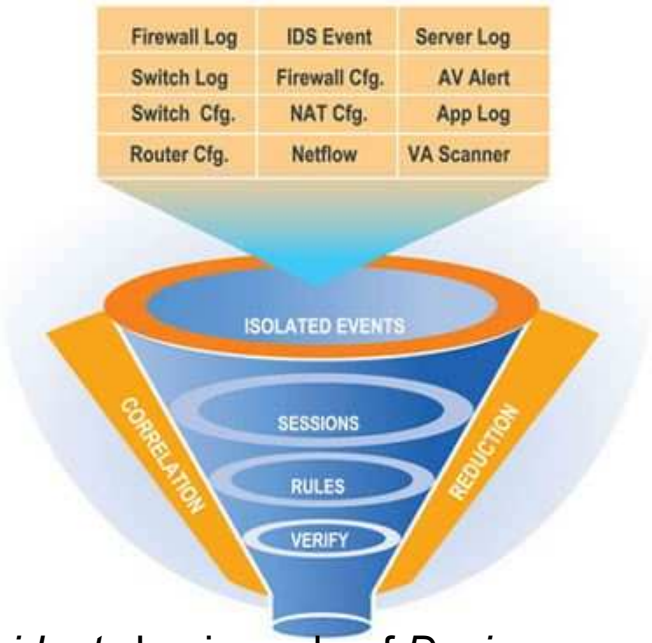


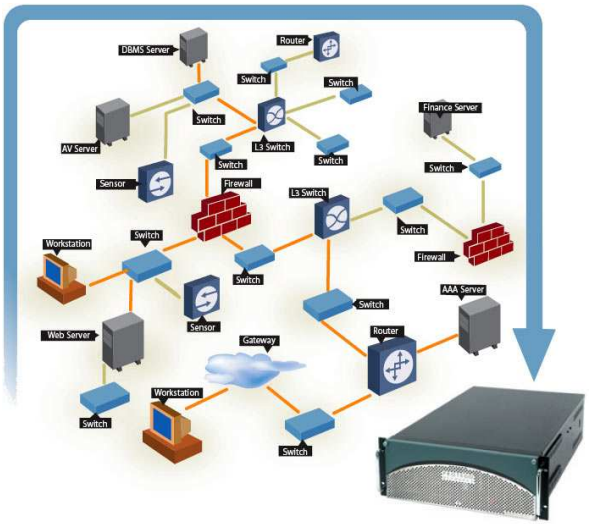
Cisco MARS
(Mitigation and Response System)

- Nutzung der vorhandenen Netzwerkinfrastruktur zur Sicherheitsanalyse
- Datenkorrellierung im kompletten Netz

  NIDS, Firewall, Router, Switches, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs
- Schnelle Lokalisierung von Angriffen und Einleitung von Gegenmaßnahmen





- Key Features

  Meldet Security *incidents* basierend auf *Device messages*, *events*, und “*sessions*”

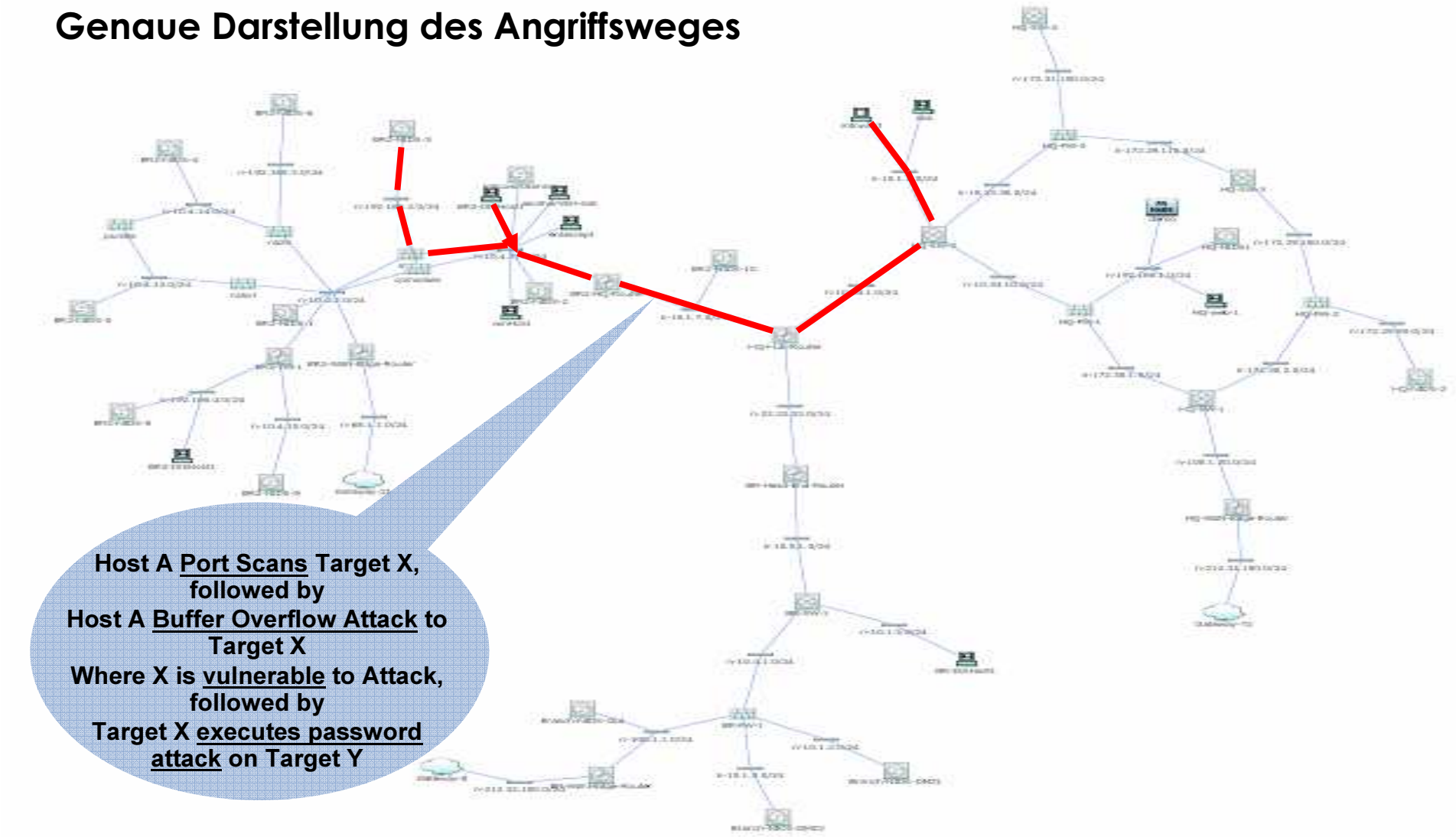
  Incidents werden graphisch in der topologie dargestellt

  Gegenmaßnahmen auf L2 ports und L3 Geräten

  Skalierbarkeit auch in komplexeren Umgebungen

CS-MARS Datenkorrelierung

Genaue Darstellung des Angriffsweges



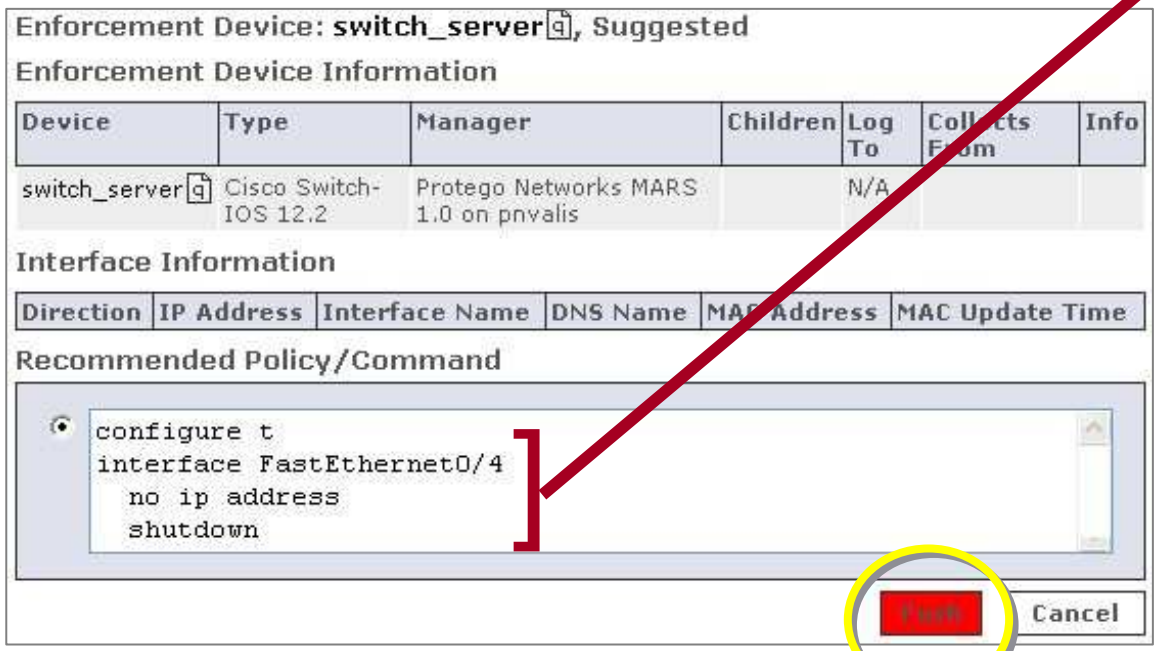
CS-MARS
Einleitung von Gegenmaßnahmen

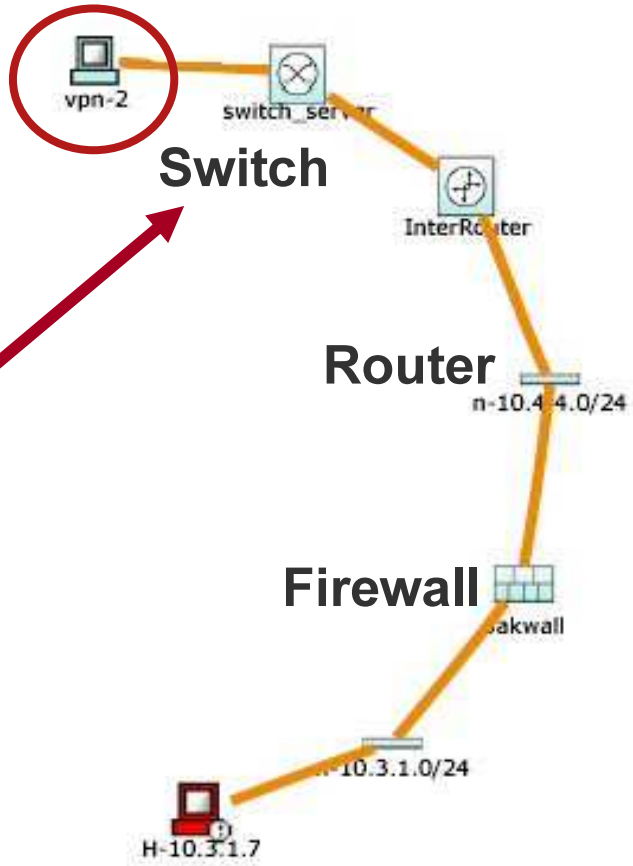
- Nutzung der Abwehrmöglicheiten innerhalb des Netzwerks

Graphische Darstellung des Layer 2–3 attack path.

Gegenmaßnahmen werden auf dem Netzwerkgerät durchgeführt.

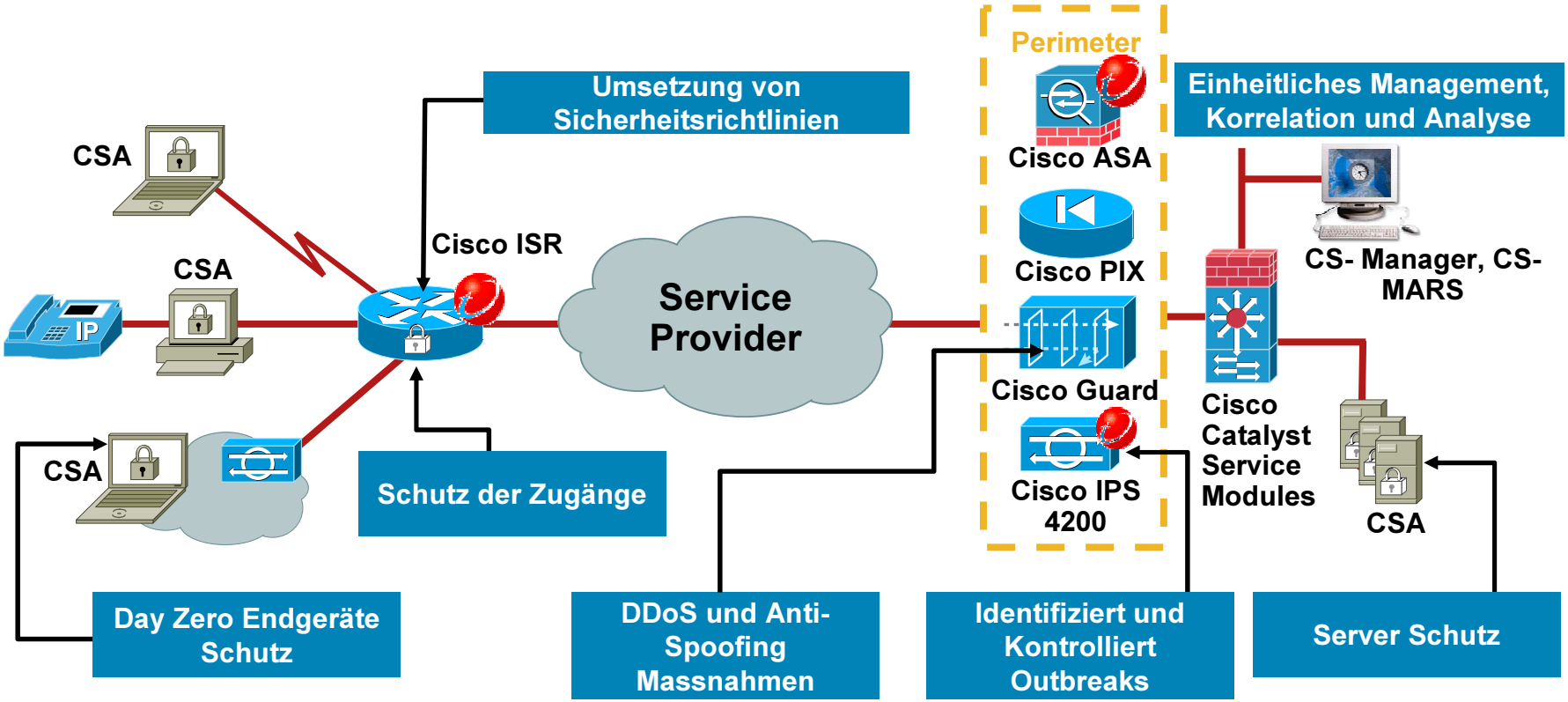
Cisco MARS konfiguriert Gegenmaßnahmen



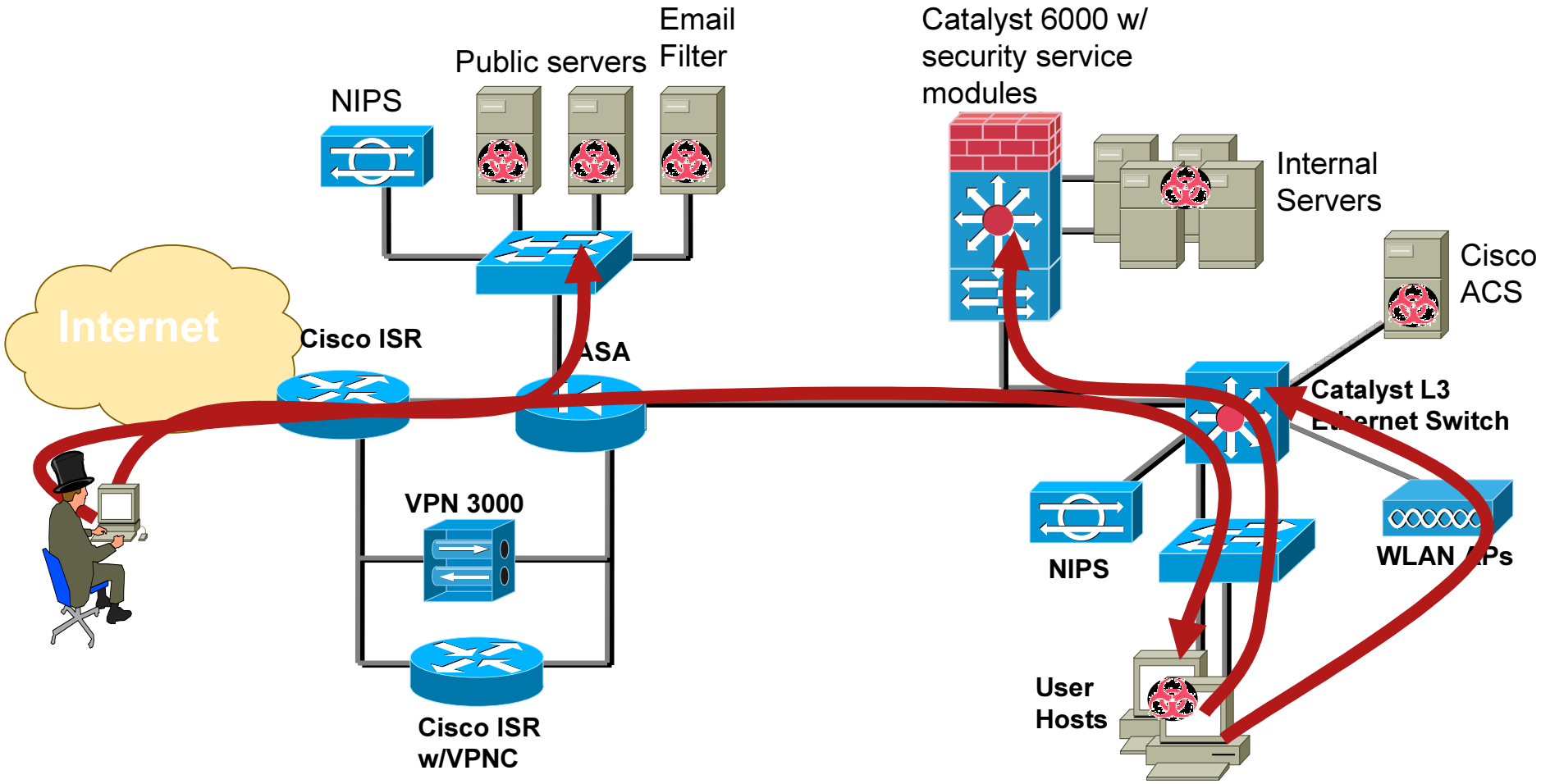


Day Zero und Intrusion Protection durchgängig im Firmennetz

Die vollständigste Intrusion Prevention Lösung am Markt

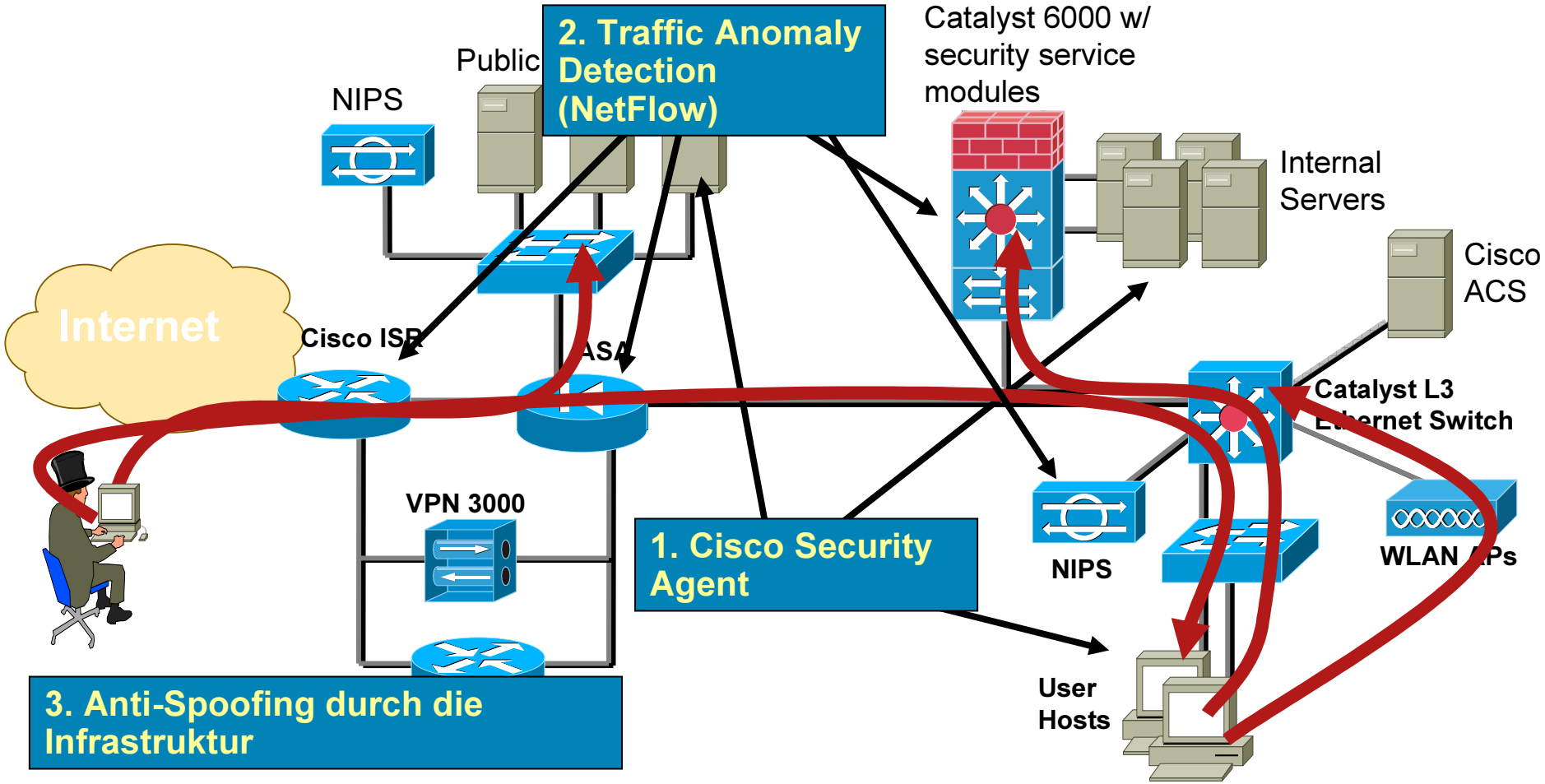


Typischer Day-Zero Angriff



Der Angriff hat einen externen Ursprung und verbreitet sich dann Intern

Day-Zero SDN Schutzmassnahmen



Zentrales Event Management (CS-MARS) bietet wichtige Informationen über die genauen Angriffspunkte und ermöglicht so wirksame Gegenmassnahmen, ausgelöst durch den Operator

Cisco Security Agent

Schutz von Stunde NULL an

Der CSA arbeitet Verhaltens-basiert!, NICHT mit Signaturen.

Eine Positivliste legt genau fest, was welche Applikation ausführen darf. Das umfasst Zugriffe auf:

- **Dateisysteme, Registry Einträge, Systemaufrufe und Systemprozesse, Installation von Software, Kommunikation über bestimmte Ports ...**

CSA bietet Schutz von Stunde Null an, da es NICHT nach den bekannten Angriffen sucht (Signatur basierend) sondern die vorhandenen Anwendungen durch Regeln schützt!