



Enterasys can secure any network from any vendor



Hubert Büsch
Diplom-Physiker
Area Sales Manager
Nordbayern (PLZ90-97)

Enterasys Networks
Solmsstraße 83
D-60486 Frankfurt am Main

Mobile + 49 172-6639916
Phone + 49 9126-287121
Fax: + 49 9126-287122
hubert.buesch@enterasys.com

www.enterasys.com

- **gegründet: 1983 (vormals Cabletron Systems)**
- **Enterprise Technology Leader: intelligenteste und sicherste Netzwerke der Welt**
- **Mehr als 900 Mitarbeiter weltweit in 30 Ländern**
- **Zwei Entwicklungszentren in Andover (USA) und Mississauga (CAN)**
- **640+ Patente, (12 im letzten Jahr)**
- **resultierend aus mehr als US \$1 Mrd. R&D Investition**
- **Mehr als 4500 Kunden in mehr als 70 Ländern**
- **85% des FORTUNE 500 zusammen mit starker Präsenz in den Märkten der öffentlichen Verwaltung, Versicherungen, Gesundheitswesen sowie der Forschung&Lehre**
- **zufriedene Kunden (über 95% der Kunden kaufen wieder Enterasys)**
- **Eigenständiges Auftreten am Markt**
- **2005 Übernahme durch The Gores Group**
- **Seit Okt.2008 Joint Venture mit Siemens SEN**



Wo Sie uns finden....

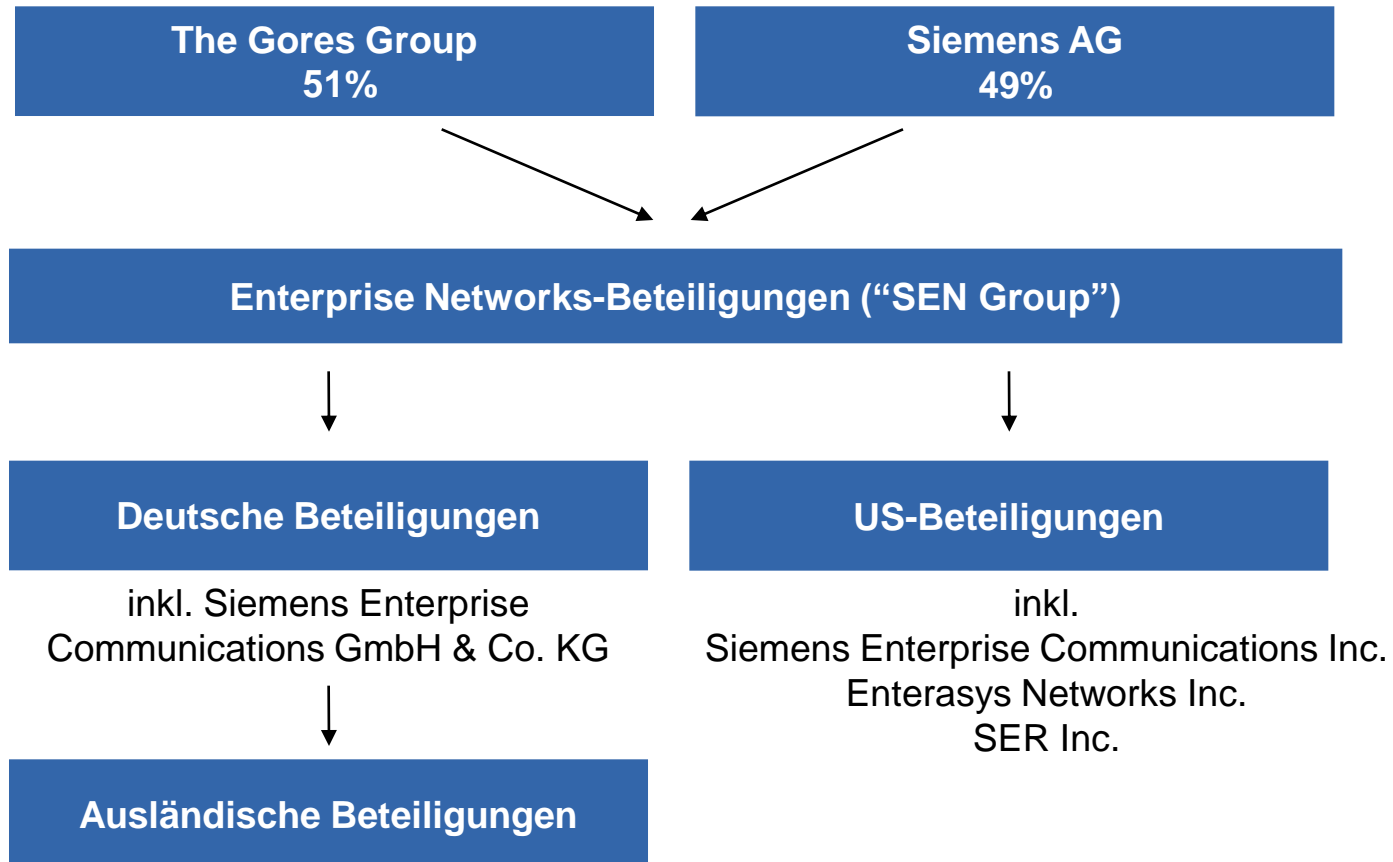


***Hauptsitz weltweit
Andover bei Boston / USA***

***Hauptsitz
CEE & APAC
Frankfurt a.M.***



Das Joint Venture: Siemens Enterprise Communications Group



Vervollständigtes Angebot und starke Basis

SIEMENS

**Unified
Communi-
cations**

- Auf dem Weg zum Software, IT- und Dienstleistungs-Geschäft
- Starke, erfahrene Partner und Führung
- Bestmögliche finanzielle Grundlagen
- Kostenoptimiert
- Ressourcen für weitere Investitionen und R&D

**Secure
Networks**



Contact Centers

- **Gäste (externe Mitarbeiter, Partnerfirmen, Techniker) im Netzwerk ?**
- **Störungen im Netzwerk, z.B. fremder dhcp-Server ?**
(dhcp-, Web-Server-, ftp-Server-Dienste können große Gefahren mit sich bringen)
- **Laptop-User**
(Vertriebsmitarbeiter connecten sich nach Tagen wieder in das Netzwerk)
(Un-)Trusted End-Systeme im Netzwerk ?
- **Sind „Produktionssysteme“ abzusichern?**
(Systeme, die keine aktuellen Patches haben, sind besonders gefährdet)
- **Möchten Sie fremde Wireless-Access-Points und Switches verhindern ?**
- **Wireless im Einsatz oder geplant ?**
- **VoIP im Einsatz oder geplant ?**
- **VPN, Firewalling, IDS/IPS im Einsatz oder geplant?**
- **Planen Sie 802.1x und nutzen Wake-on-LAN?**

1. **Detection** (Inventarisierung der Endgeräte)

2. **Authentication** (802.1x, MAC+Kerberos, Web...)

3. **Assessment** (Scannen der Endgeräte)

4. **Authorization** (ja/nein, VLAN, Policy)

5. **Remediation** (Heilung, Information)

Detect

Authenticate

Remediat.

Assess

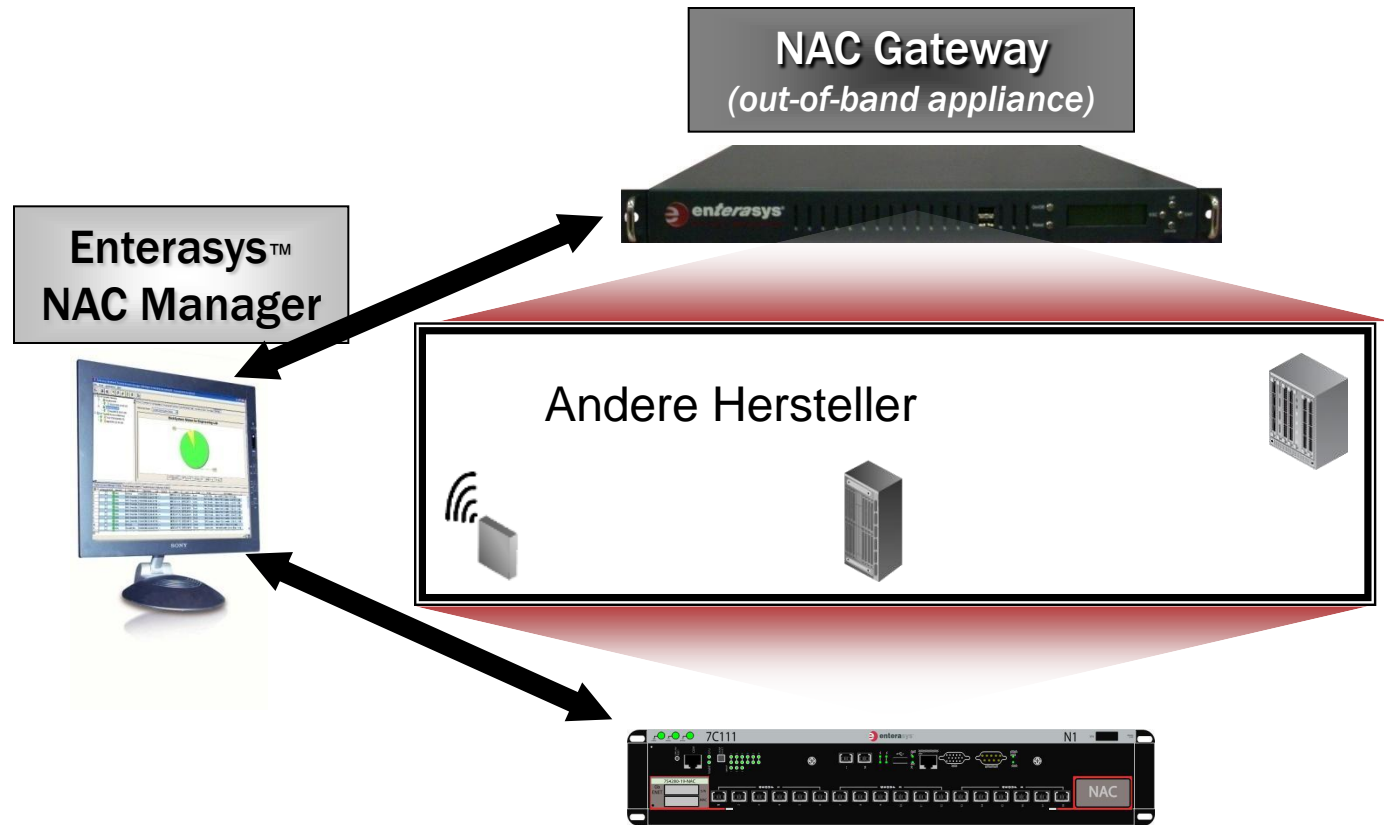
Authorize



pre-connect NAC defined

Pre-connect NAC Functions:

1. **Detection**
2. **Authentication**
3. **Assessment**
4. **Authorization**
5. **Remediation**

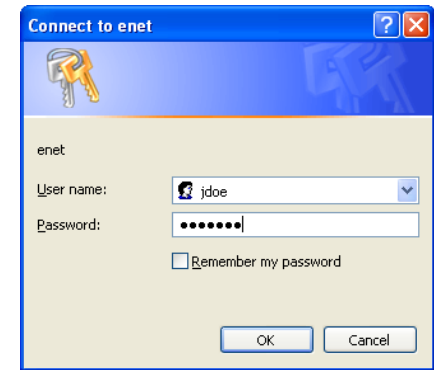


NAC-Gateways stehen im Authentifizierungsstrom

NAC-Controller (=NAC-Gateway+Switch) stehen zusätzlich im Datenstrom. Dadurch zusätzliche Policy-Möglichkeiten

—End-User Authentication

- < End user must enter a valid username and password to successfully register a device
- < Username/password validated against a backend LDAP server (e.g. MS Active Directory, OpenLDAP, etc.)



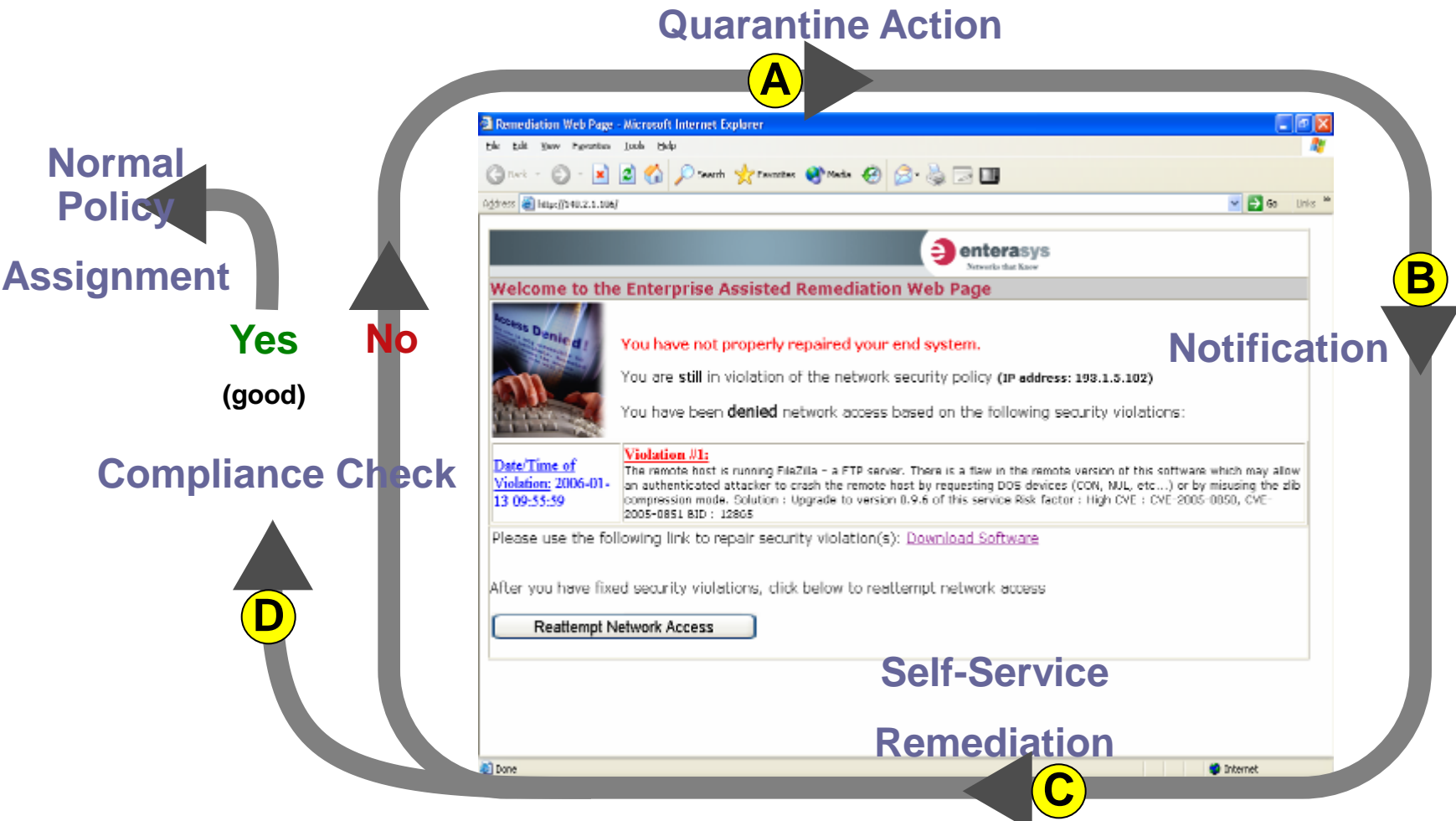
—Sponsored Registration

- < End user must be in the presence of a trusted employee (i.e. sponsor) to successfully register a device
- < Sponsor username/password validated against backend LDAP server, OR sponsor accounts configured in NAC manager

—MAC Reg Web Admin Interface

- < Supports bounded visibility and control into MAC Reg system
 - View, edit, add, delete registered end systems
 - Useful for HelpDesk access into system without mandating HelpDesk access to NAC manager
- < Located at https://NAC_Gateway/administration.php
- < “Sponsor Web Admin” Interface is supported so spons





- The load on the help desk support group should not increase as a result of the quarantine
- A universal function is the remediation webpage, WMI can be used too
- Auto Remediation is desired

Open Communication Solution for Location and Identity Assurance: data exchange

- The exchanged data is presented as additional endsystem data in the NAC Manager but also on the HiPath DLS

Enterasys NMS NAC Manager: Endsystem View

	NAC Appliance	MAC Address	Switch IP	Switch Location	Switch Port Index	Switch Port	Host Name	Operating System	IP Address
1	NAC Controller PDP/172.1...	SIEMENS :10:1F:3C	172.16.90.30	ISBLab FFM	12014	ge.1.14	43254	OpenStage 80:V1 R4.14	172.16.90.120
2	NAC Controller PDP/172.1...	02:01:02:03:00:05	172.16.90.30	ISBLab FFM	12013	ge.1.13			
3	NAC Controller PDP/172.1...	SIEMENS :10:1F:C4	172.16.90.30	ISBLab FFM	12013	ge.1.13	43255	OpenStage 80:V1 R4.14	172.16.90.121
4	NAC Controller PDP/172.1...	INTEL CO:95:C0:72	172.16.90.30	ISBLab FFM	12001	SWitch_LINKS ("ge.1.1")	wk1	Windows XP	172.16.90.150
5	NAC Controller PDP/172.1...	CISCO SY:4A:A1:C0	172.16.90.30	ISBLab FFM	12001	SWitch_LINKS ("ge.1.1")			
6	NAC Controller PDP/172.1...	INTEL CO:66:73:DE	172.16.90.30	ISBLab FFM	12001	SWitch_LINKS ("ge.1.1")		Windows XP	172.16.90.157
7	NAC Controller PDP/172.1...	CISCO SY:4A:A1:99	172.16.90.30	ISBLab FFM	12001	SWitch_LINKS ("ge.1.1")			

Device phone number
(e.g. 43254)

Device Type and SW version
(e.g. OpenStage 80:V1 R4.14.0)

DLS IP Infrastructure

IP Switch Daten	
Infrastruktur Policy:	Hamburg Voice
Switch Name:	PerformanceTest
Switch Standort:	TestLAB
Switch IP Adresse:	172.16.90.22
Switch Port:	ge.1.9
Port Alias:	alias:9
Port ELIN:	1124321
Network Policy:	IPPhone
Remediation Info:	ACCEPT
Gerätestatus:	unbekannt

Software: NetSight NAC-Manager

- **NS-AB-50** NetSight Advanced Bundle 50-devices (50 device Console license for 1 server plus 3 concurrent users with Policy Manager, Policy Control Console, Automated Security Manager, Inventory Manager, and NAC Manager), für Neukunden gibt es eine Promotion

Hardware: NAC-Gateways

- **SNS-TAG-LPA** SENTINEL LOW END APPLIANCE - 2000 USER SUPPORT
- **SNS-TAG-HPA** SENTINEL HIGH END APPLIANCE - 3000 USER SUPPORT
- **SNS-TAG-ITA** NAC Gateway, 3000 user, supports available add-on assessment license

Assessment (SNS-TAG-ITA or NAC-Controller required):

- **NAC-ASSESS-LIC** integrated agent based and agentless assessment option for the SNS-TAG-ITA and the AND 2S4082-25/ 7S4280-19-SYS

2S4082-25-SYS – 12 Gbit/s, up to 1024 users



7S4280-19-SYS – 18,5 Gbit/s, up to 1024 users



Support für Kerberos Snooping und Policing

2S4082-25-SYS 24-PORT 10/100/1000 NAC CONTROLLER

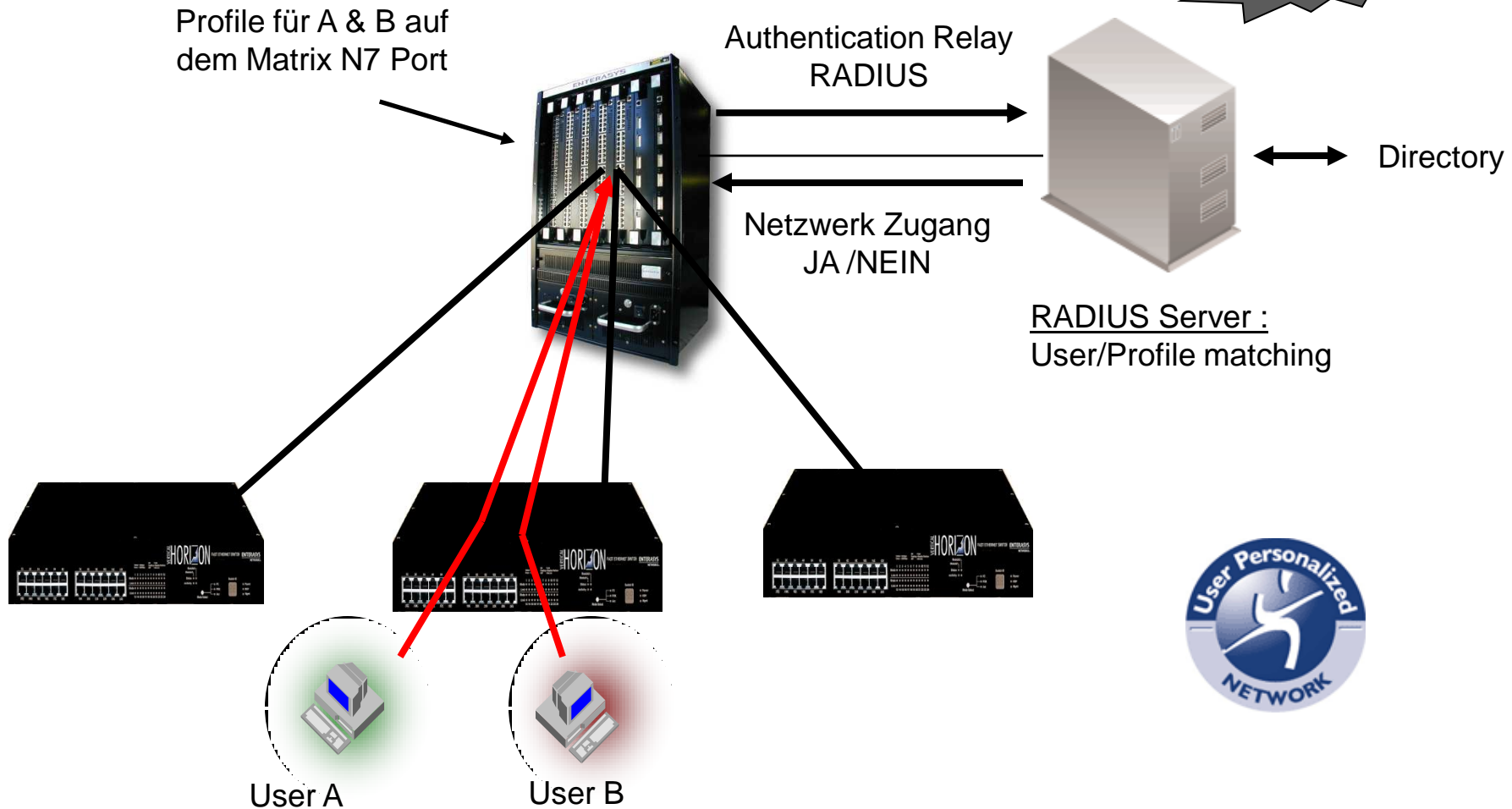
7S4280-19-SYS 20-PORT SFP NAC CONTROLLER

- Detection Mode des NAC-Gateways inkl. Kerberos Snooping, Erkennen von Endgeräten: MAC-, IP-Adressen, Username, Rechnername an welchem Port zu welcher Zeit, IP-Phones, automatische Inventarisierung, Übersetzung des Vendor-Codes. Damit kann Authentifizierung später viel schneller umgesetzt werden.
- Radius-Authentifizierung für die MAC-Adressen im NAC-Gateway, Radius-Proxy für 802.1x und Web (Somit müssen die MAC-Adressen nicht mühsam in das active directory eingetragen werden).
- Das NAC-Gateway entdeckt neue MAC-Adressen automatisch und informiert den Netzwerkmanager. Dieser entscheidet nur noch, welchen Zugriff das Gerät bekommt. Das Enterasys-NAC-Gateway fragt das Endgerät über eine eingeblendete Web-Page nach persönlichen Daten.
- Komplette Hot-Spot-Lösung für Gäste
- Keine Kosten für die NAC-Clients, (man muss sich nicht um Lizenzen kümmern)
- Assessment mit und ohne Agent auf dem Client. Somit können auch Gäste ohne Agent gescannt werden.
- Remediation (automatische „Heilung“ des Endgerätes mit Benachrichtigung des Benutzers), sowohl agent-based als auch agent-less.
- Jahrelange Assessment-Erfahrung in heterogensten Umgebungen, z.B. University of North Carolina mit 40.000 Studenten
- Prüfung auf allerneueste Vulnerabilities, auch für die es noch kein Patch gibt.

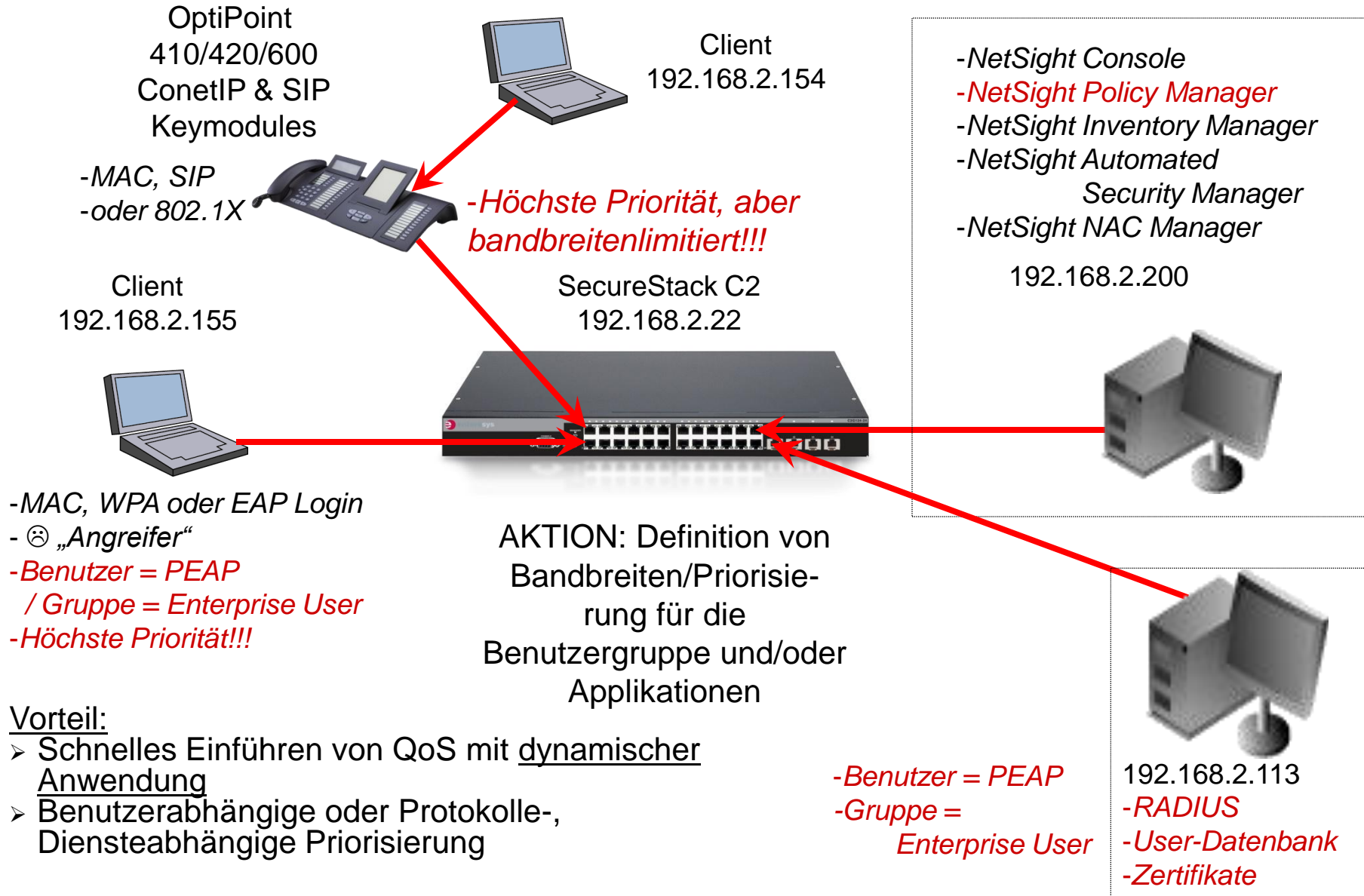
Multi-MAC based Authentication und Policing

Advanced

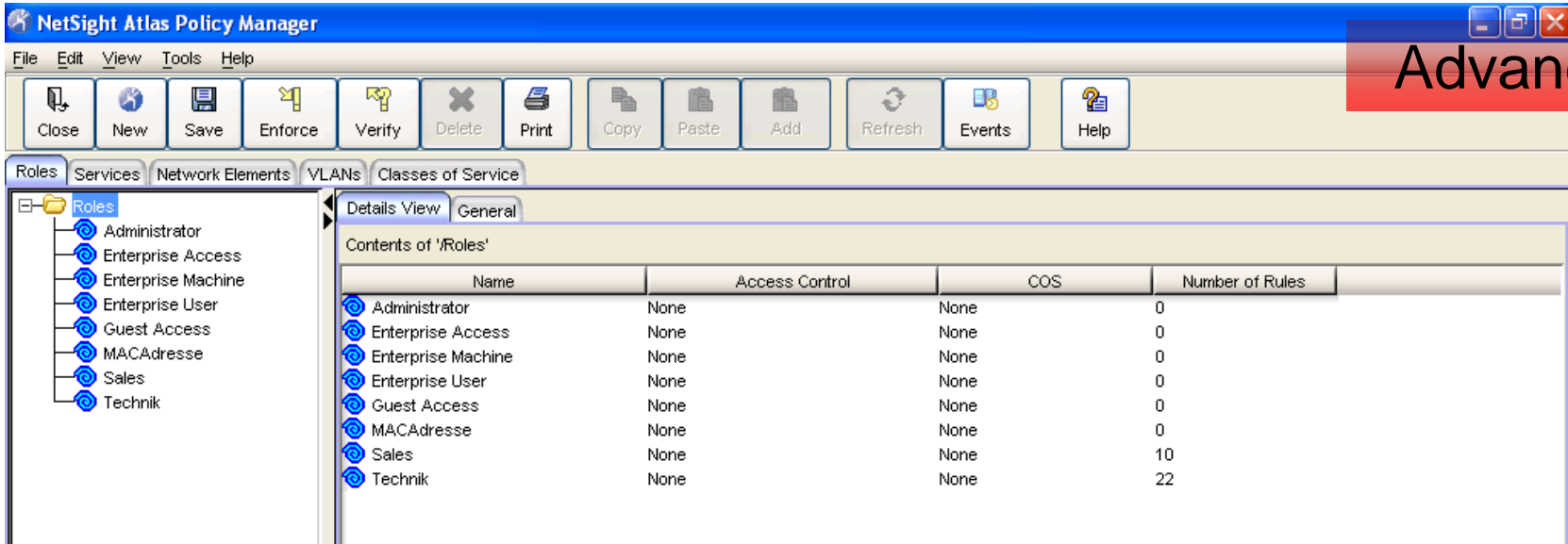
Platinum



Sicheres Netzwerk für zusätzliche Anwendungen / Bandbreitenmanagement Dual-User-Authentication bei SecureStack C (B und D mit Policy-Upgrade)



Rollen-basierte Administration



NetSight Atlas Policy Manager

File Edit View Tools Help

Close New Save Enforce Verify Delete Print Copy Paste Add Refresh Events Help

Roles Services Network Elements VLANs Classes of Service

Roles

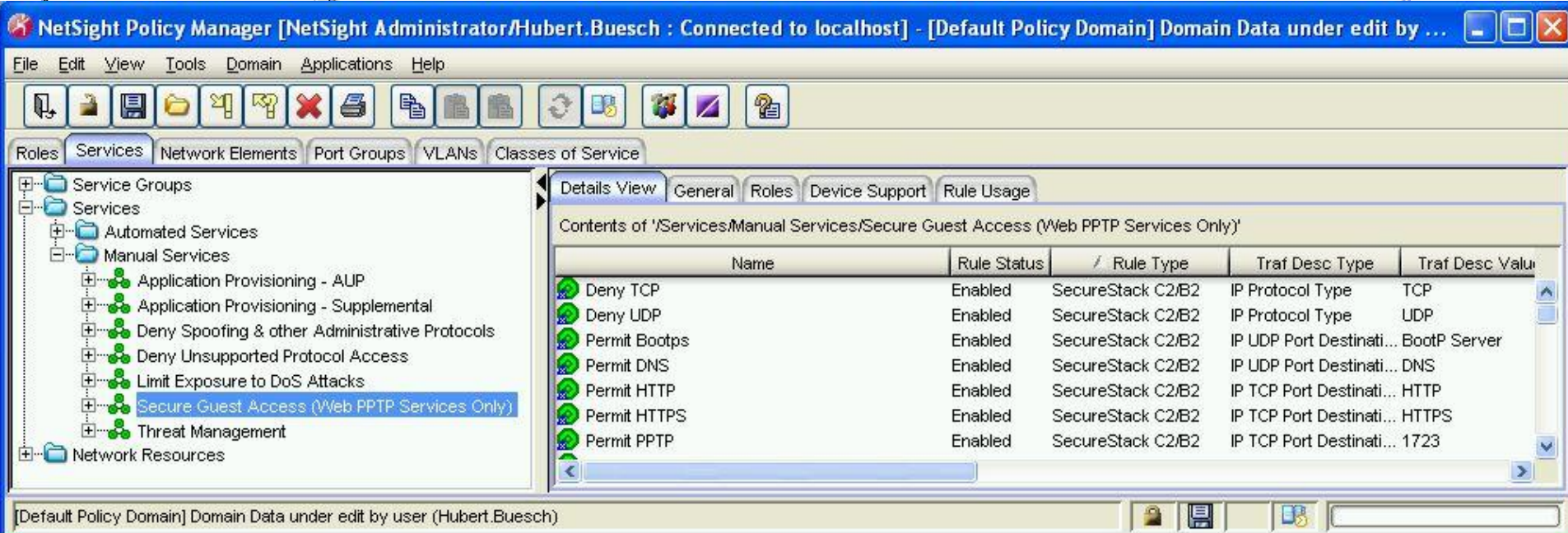
- Administrator
- Enterprise Access
- Enterprise Machine
- Enterprise User
- Guest Access
- MACAdresse
- Sales
- Technik

Details View General

Contents of 'Roles'

Name	Access Control	COS	Number of Rules
Administrator	None	None	0
Enterprise Access	None	None	0
Enterprise Machine	None	None	0
Enterprise User	None	None	0
Guest Access	None	None	0
MACAdresse	None	None	0
Sales	None	None	10
Technik	None	None	22

Advanced



NetSight Policy Manager [NetSight Administrator/Hubert.Buesch : Connected to localhost] - [Default Policy Domain] Domain Data under edit by ...

File Edit View Tools Domain Applications Help

Roles Services Network Elements Port Groups VLANs Classes of Service

Service Groups

- Services
 - Automated Services
 - Manual Services
 - Application Provisioning - AUP
 - Application Provisioning - Supplemental
 - Deny Spoofing & other Administrative Protocols
 - Deny Unsupported Protocol Access
 - Limit Exposure to DoS Attacks
 - Secure Guest Access (Web PPTP Services Only)
 - Threat Management
- Network Resources

Details View General Roles Device Support Rule Usage

Contents of '/Services/Manual Services/Secure Guest Access (Web PPTP Services Only)'









Name	Rule Status	Rule Type	Traf Desc Type	Traf Desc Valu
Deny TCP	Enabled	SecureStack C2/B2	IP Protocol Type	TCP
Deny UDP	Enabled	SecureStack C2/B2	IP Protocol Type	UDP
Permit Bootps	Enabled	SecureStack C2/B2	IP UDP Port Destinati...	BootP Server
Permit DNS	Enabled	SecureStack C2/B2	IP UDP Port Destinati...	DNS
Permit HTTP	Enabled	SecureStack C2/B2	IP TCP Port Destinati...	HTTP
Permit HTTPS	Enabled	SecureStack C2/B2	IP TCP Port Destinati...	HTTPS
Permit PPTP	Enabled	SecureStack C2/B2	IP TCP Port Destinati...	1723

[Default Policy Domain] Domain Data under edit by user (Hubert.Buesch)

- FST bietet schutz vor Angriffen
- Es werden pro Port die Anzahl der Flows gezählt
 - Zwei Flow Count ActionLimits (ActionLimit1 & ActionLimit2)
 - < “ActionLimit” Feld definiert die Anzahl der Flows wann entsprechende “ActionTaken” eintritt
 - < Das zweite Limit ist für größere Flexibilität. Typischerweise, das erste Limit für eine Warnung, das zweite Limit für eine automatische Handlung
 - Zwei Flow Count Actions (ActionTaken1 & ActionTaken2)
 - < Das ActionTaken Feld beschreibt die Aktion welche hervorgerufen werden soll, wenn das Limit der Flows überschritten wird.
 - < Beispiel:
 - ActionLimit1 = 200; ActionTaken1 = GenerateNotification
 - ActionLimit2 = 800; ActionTaken2 = GenerateNotification & DisableInterface
 - < Ursache von vielen Flows sind meist Hacker-Tools oder Wurm/Virus





Enterasys Product Portfolio: Security-Enabled Infrastructure



Product	Application	Scaling	Features	Key Benefits
 Matrix X	Routing for large LAN cores and high performance data centers	<ul style="list-style-type: none"> • 128 10GE ports • 512 GE ports • 476 Mpps throughput 	<ul style="list-style-type: none"> • Three chassis options • Full featured IP routing • Non-stop architecture • Advanced QoS and control 	<ul style="list-style-type: none"> • Carrier class high availability • Industry leading performance and density • Security for core of network
 Matrix N	Routing and switching for LAN distribution, edge and small core and Virtual Data Center deployments	<ul style="list-style-type: none"> • 28 10GE ports • 504 PoE end user ports • 94.5 Mpps 	<ul style="list-style-type: none"> • Four chassis options • Distributed flow based switching for powerful security policy capabilities • Multi-user authentication • Optional Dragon modules 	<ul style="list-style-type: none"> • Industry leading comprehensive network based security solution • Network high availability • Dynamic security/QoS eases management and mobility
 SecureStack A / B / C	LAN Edge L2/L3 stackable switching solutions	<ul style="list-style-type: none"> • Up to 8 units in a stack • 384 end user ports up to Gigabit speeds 	<ul style="list-style-type: none"> • Flexible 10/100, triple speed, PoE, GigE, and 10GE configurations • Policy enabled (B & C) • Multiple auth options 	<ul style="list-style-type: none"> • Limited lifetime warranty and ease-of-use lowers total cost of ownership • Extends Secure Networks to network edge
 SecureSwitch D	Compact, quiet L2 edge switch for classroom and office environments (Q1'08)	<ul style="list-style-type: none"> • 12 end user 10/100/1000 ports • Optional PoE 	<ul style="list-style-type: none"> • Policy enabled switch • Quiet operation • Extended environmental range for up to 60°C 	<ul style="list-style-type: none"> • Cost effective solution for Secure Networks in classroom and office environments • Limited Lifetime Warranty
 SecureSwitch G	Fixed/modular high density L2/3 LAN edge switch, smaller distribution, (Q1 08)	<ul style="list-style-type: none"> • Up to 96 end user ports • Up to 12 10GE • PoE options 	<ul style="list-style-type: none"> • Line rate switching/routing • Integrated security policy • Redundant power • 15.4W PoE power - all ports 	<ul style="list-style-type: none"> • Low cost, high density high availability high performance • Flexible configurations – grow as needed including PoE
 SecureSwitch I	Edge switching for industrial applications	<ul style="list-style-type: none"> • Up to 24 end user 10/100 ports 	<ul style="list-style-type: none"> • Policy enabled L2 switching • Robust design for harsh industrial environments • Flexible configurations 	<ul style="list-style-type: none"> • Secure networking for critical industrial applications • Easy switch replacement by non-technical personnel
 RoamAbout Wireless	Wireless networking infrastructure	<ul style="list-style-type: none"> • Up to 120 Access Points controlled by a single switch 	<ul style="list-style-type: none"> • Policy enabled wireless • “Thick” & “Thin” options • 802.11n capable • WiFi rogue detection 	<ul style="list-style-type: none"> • Only solution to fully integrate wireless infrastructure into security policy architecture • Integrated thick and thin APs
 XSR Branch Router	Security router for branch office	<ul style="list-style-type: none"> • Up to 2 Gbps, 3000 VPN tunnels 	<ul style="list-style-type: none"> • Firewall, VPN, ADSL, 10/100 Ethernet 	<ul style="list-style-type: none"> • Strong security for branch • High performance and capacity • Low cost – long service

Enterasys Product Portfolio: Advanced Security & Management Applications



Product	Application	Features	Key Benefits
 <p>Dragon Security Command Console (DSCC)</p>	<p>Security Information and Event Manager (SIEM) which integrates and analyzes security information from multiple sources</p>	<ul style="list-style-type: none"> • Gathers, correlates, and prioritizes network security information • Automates report generation for security compliance auditing 	<ul style="list-style-type: none"> • Eases compliance validation • Reduces overload of network security data • Enhances visibility and control • Expedites responses to detected malicious behavior
 <p>Network Access Control</p>	<p>Standards-based application securing network access prior to and after connecting in a multi-vendor network</p>	<ul style="list-style-type: none"> • Ensures compliance to network security policies • Operates in any network without forklift upgrades • Includes centralized management and control 	<ul style="list-style-type: none"> • Continuous business protection minimizes costs from security threats • Investment protection • IT Operations efficiency
 <p>Dragon Intrusion Defense</p>	<p>Suite of appliances and applications which actively monitor network traffic to detect and prevent security threats</p>	<ul style="list-style-type: none"> • High performance network based sensors monitor traffic in real time • Host based sensors protect individual end systems • Advanced threat detection algorithms identify known and unknown threats 	<ul style="list-style-type: none"> • Provides real-time detection and response to active network threats • Minimizes impact and costs of any security threats on the network
 <p>NetSight</p>	<p>Integrated portfolio of network and security management applications</p>	<ul style="list-style-type: none"> • Centralizes configuration and control of network devices • Automates security enforcement on network infrastructure • Open standards based architecture 	<ul style="list-style-type: none"> • Reduces costs of managing, controlling, and planning complex networks • Increases business productivity by reducing the time to troubleshoot and repair network problems

- **NetSight Console**
 - System Konfiguration (Ports, Vlans, Autoneg, ...)
 - Compass (Wo ist IP, MAC, User, hostname ...)
 - Topologieansicht
 - Überwachung
 - FlexViews
 - Alarm Management
 - Gruppierungen Devices, Lokationen, Benutzer-definiert,...
 - MIB Tools
- **NetSight Inventory Manager**, Inventarisierung der Netzwerkkomponenten und deren Configs
- **NetSight Policy Manager** (für Policy enabled Enterasys-Switches)
- **NetSight NAC Manager** (im Zusammenspiel mit NAC-Gateways/NAC-Controller)
- **NetSight Automated Security Manager (ASM)**
- **Dragon Intrusion Detection & Prevention (IDS/IPS) / Dynamic Intrusion Response (DIR)**
- **Dragon Security Command Console (DSCC) = Security Information & Event Management (SIEM)**



enterasys[®]
Secure Networks[™]

Thank You

