enterasys™
Networks that Know

# La Sicurezza Vive nella Rete: Policy-Enabled Network

Mauro Rossi
Pre-Sales Engineer

7one SOLUTION

Il Panorama della Sicurezza e' Cambiato Drammaticamente

Networks Sono Sotto Attacco

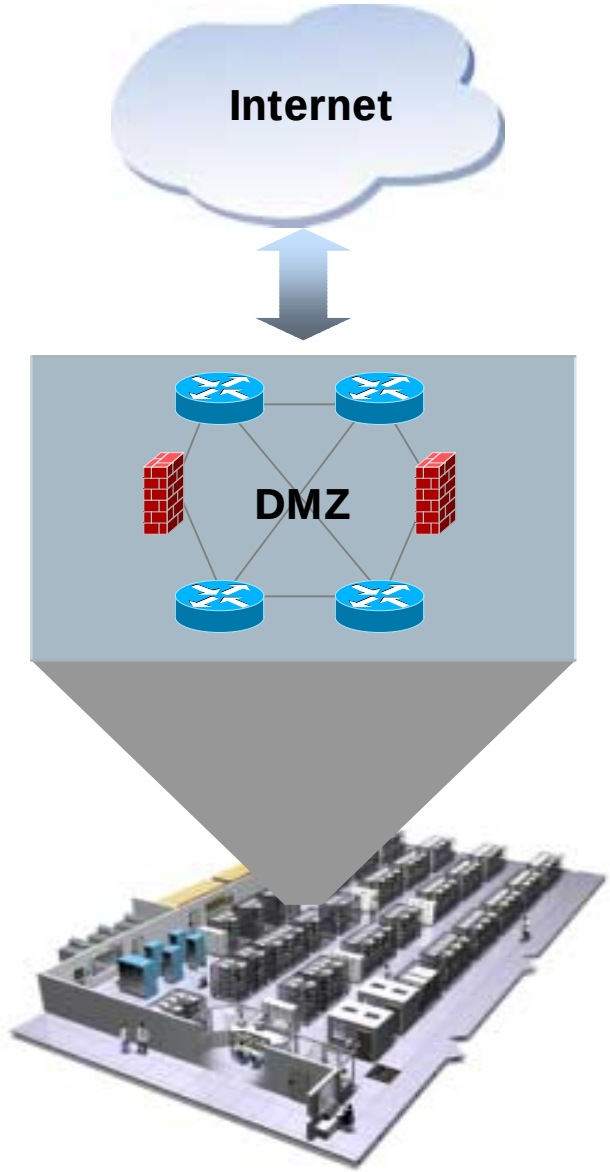
Attuali Infrastrutture di Rete e di Sicurezza devono Essere Migliorate

*Nel 2004, Worms che Impiegavano Parecchi Giorni per Attraversare il Mondo , hanno Colpito più di 300,000 Sistemi in Sei Continenti in Meno di 15 Minuti dalla loro Esecuzione*

***"Ognuna di queste minacce ha origine in un punto qualsiasi della rete e attraverso la rete si diffonde "***

# Come proteggere la Rete

- **La soluzione tradizionale per la sicurezza di rete**
  - Zona “demilitarizzata” (DMZ) tra Internet e la rete aziendale
  - Controllo e filtraggio del traffico (Firewalls)
  - Controllo e segnalazione dei tentativi di intrusione (IDS)
  - Controllo degli accessi (in ingresso e in uscita)
- **E’ una strategia consolidata per la connessione ad Internet che:**
  - Riduce in modo significativo gli attacchi dall’esterno verso l’interno
  - E’ utilizzata da tutte, o quasi, le aziende
- ***Ma…..* Il modello di protezione perimetrale non e’ piu’ sufficiente**



# Proteggere il Business

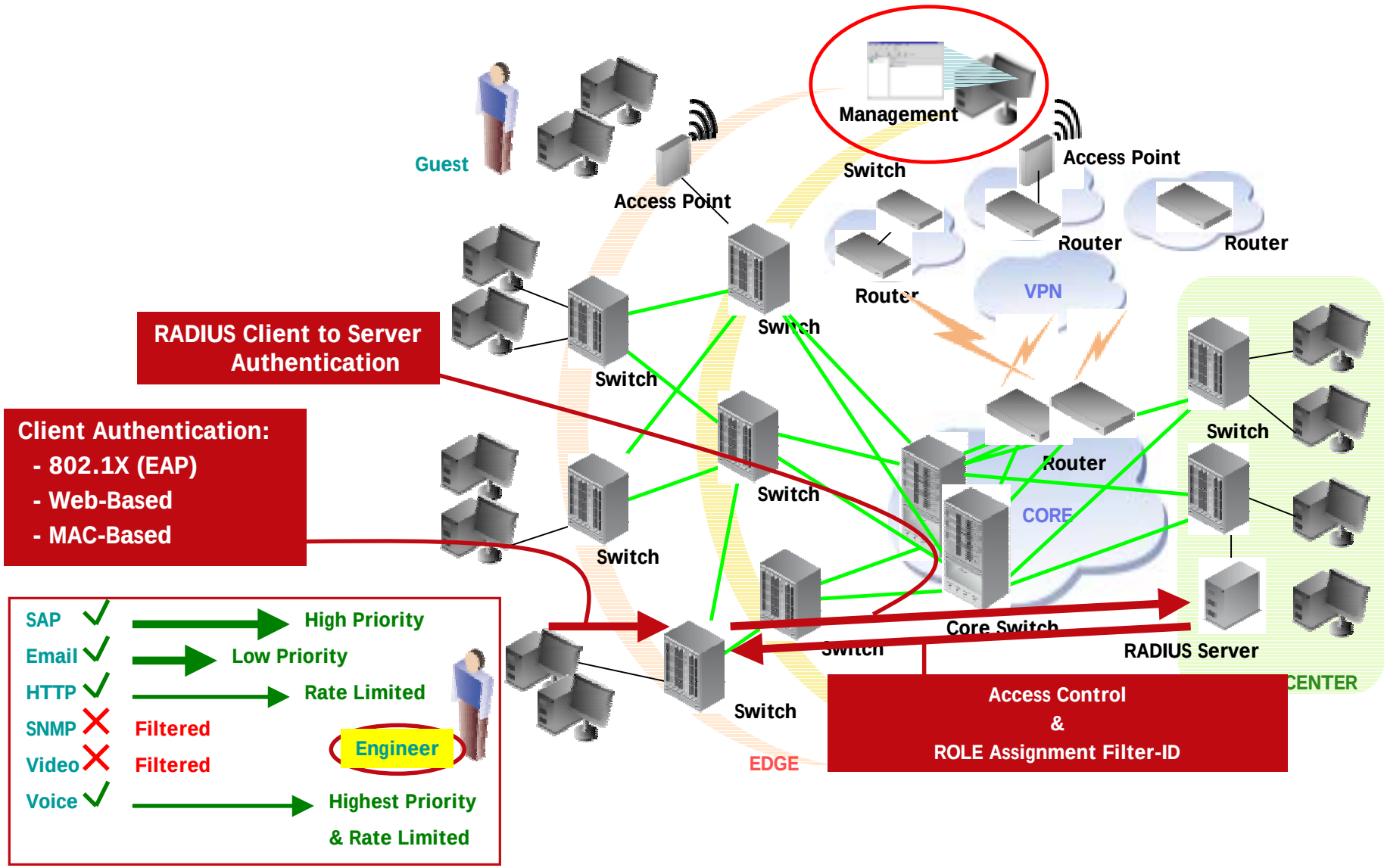
La rete non deve essere più vista come una componente “passiva”, proprio per la sua estensione e ramificazione deve essere un attivo partecipante nel veicolare la sicurezza ovunque.

- E’ necessario poter **IDENTIFICARE** ogni utente che accede alla rete, in OGNI suo punto
- Le Policies di Sicurezza devono essere applicate in ogni punto di accesso della rete
- Cambiamenti alle politiche di sicurezza devono essere rapidi e applicabili ovunque
- Intrusion detection deve essere accurata
- La sorgente di ogni minaccia deve essere identificata e localizzata velocemente
- Le azioni intraprese devono essere tempestive ed efficaci

# Integrated Security Features

- Centralized Management
- User Identity Services
- Traffic Control
- Resiliency
- Technology Specific

# Policy-Enabled Network: Access Control



# Policy-Enabled Network Authentication

- **Multiple (PWA+, MAC, 802.1X) authentication types allowed per port**
  - More than one type can be active simultaneously

- **802.1x based Authentication** (MD5,PEAP,EAP-TLS,EAP-TTLS)

- **MAC based Authentication**
  - Allow authorized MAC addresses to access the network
    - By defining the "NAS-IP-Address" and "NAS-Port" per user (MAC address) as "Check Attributes" in RADIUS, it is possible to restrict the mobility of the MAC address to a single device ("NAS-IP-Address") or to a single port ("NAS-IP-Address+NAS-Port").

- **Web based Authentication (PWA+)**
  - Unauthenticated users will have their browser session on port 80 redirected to a login page generated by the switch.

## Policy-Enabled Network

- Binds network security “policies” to a user’s role
- A single policy can combine many control elements
  - **Filtering, VLAN assignment/containment, QoS, Rate Limiting**

# Frame Classification and Action

## Layer 2 Data Link

Ethertype
DSAP/SSAP
MAC Address Source, MAC Address Destination, MAC Address Bilateral

## Layer 3 Network

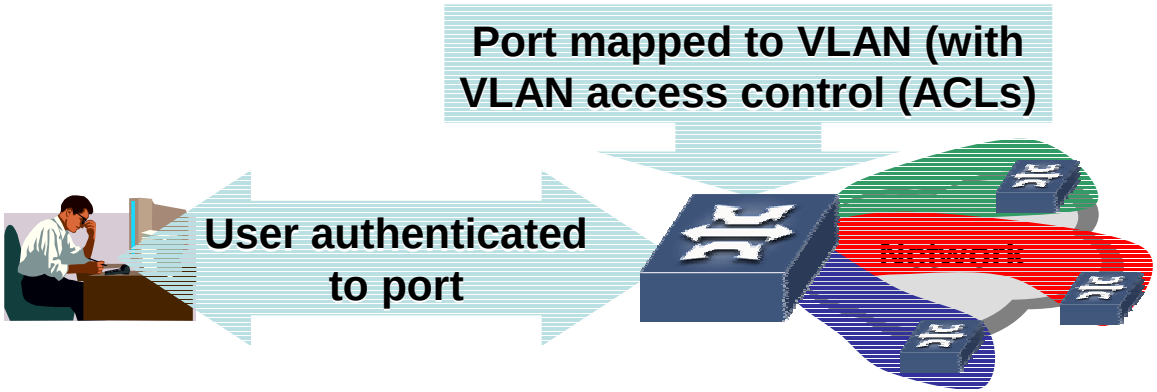
IP Type of Service
IP Protocol Type
IP Address Source, IP Address Destination, IP Address Bilateral
IP Socket Source, IP Socket Destination, IP Socket Bilateral
IP Fragment
ICMP

## Layer 4 Transport

IP UDP Port Source, IP UDP Port Destination, IP UDP Port Bilateral
IP TCP Port Source, IP TCP Port Destination, IP TCP Port Bilateral
IP UDP Port Source Range, IP UDP Port Destination Range, IP UDP Port Bilateral Range
IP TCP Port Source Range, IP TCP Port Destination Range, IP TCP Port Bilateral Range

# Single User Access and Policy Application

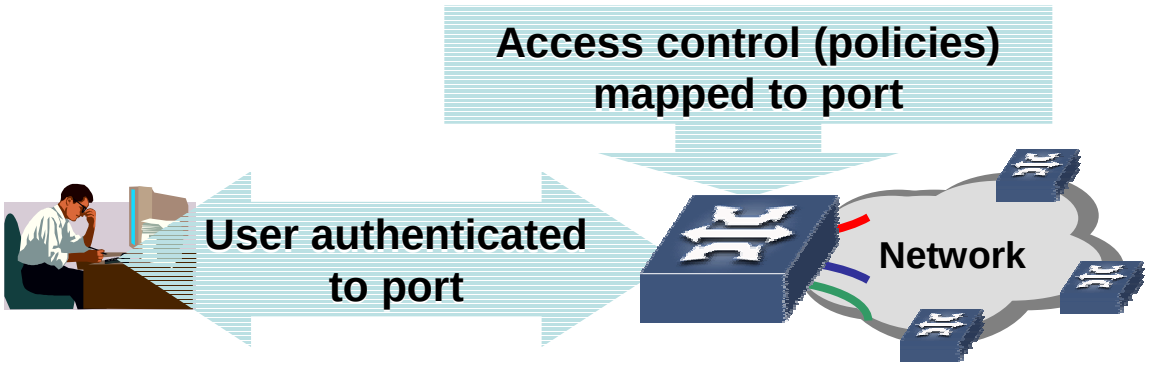
## Using VLANs (with ACLs)




### Issues

- Costly, time-consuming VLAN management
- Access control is limited to VLANs
- VLANs provide no inherent security

## Using Policies (directly)

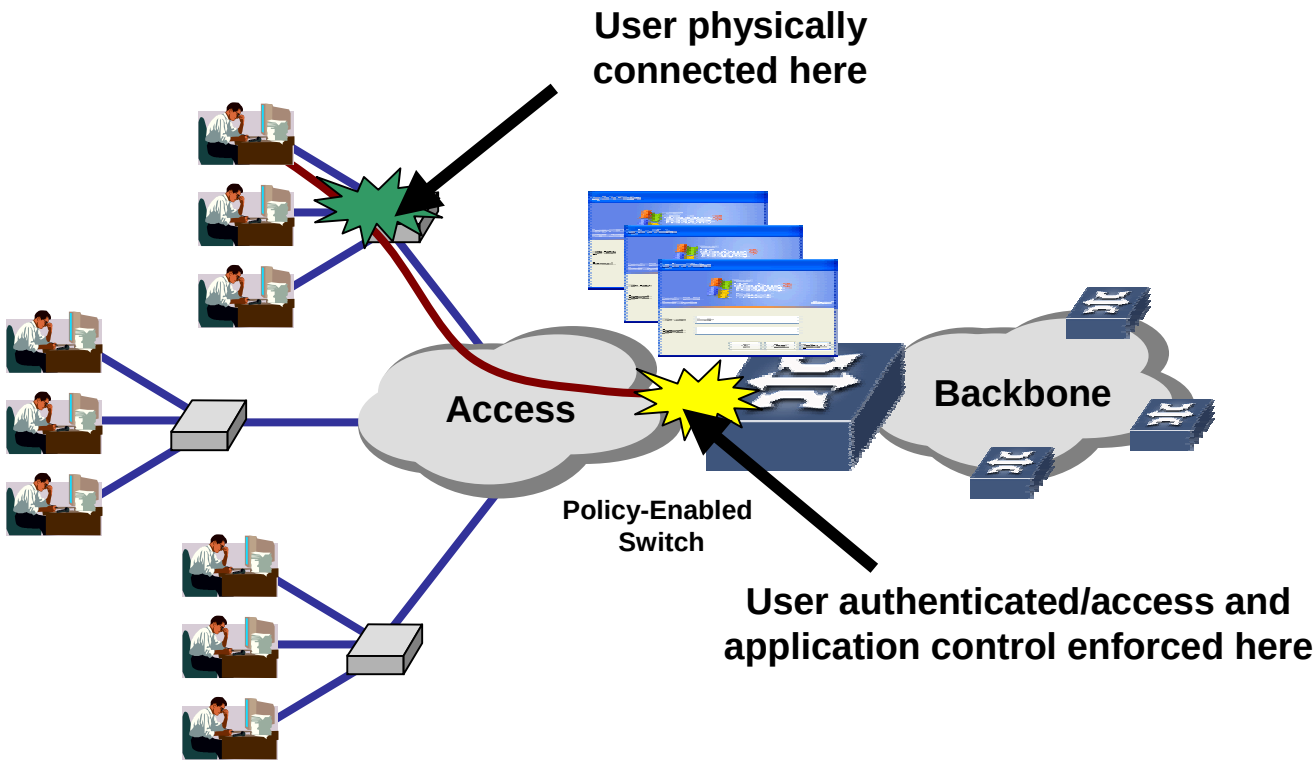



### Benefits

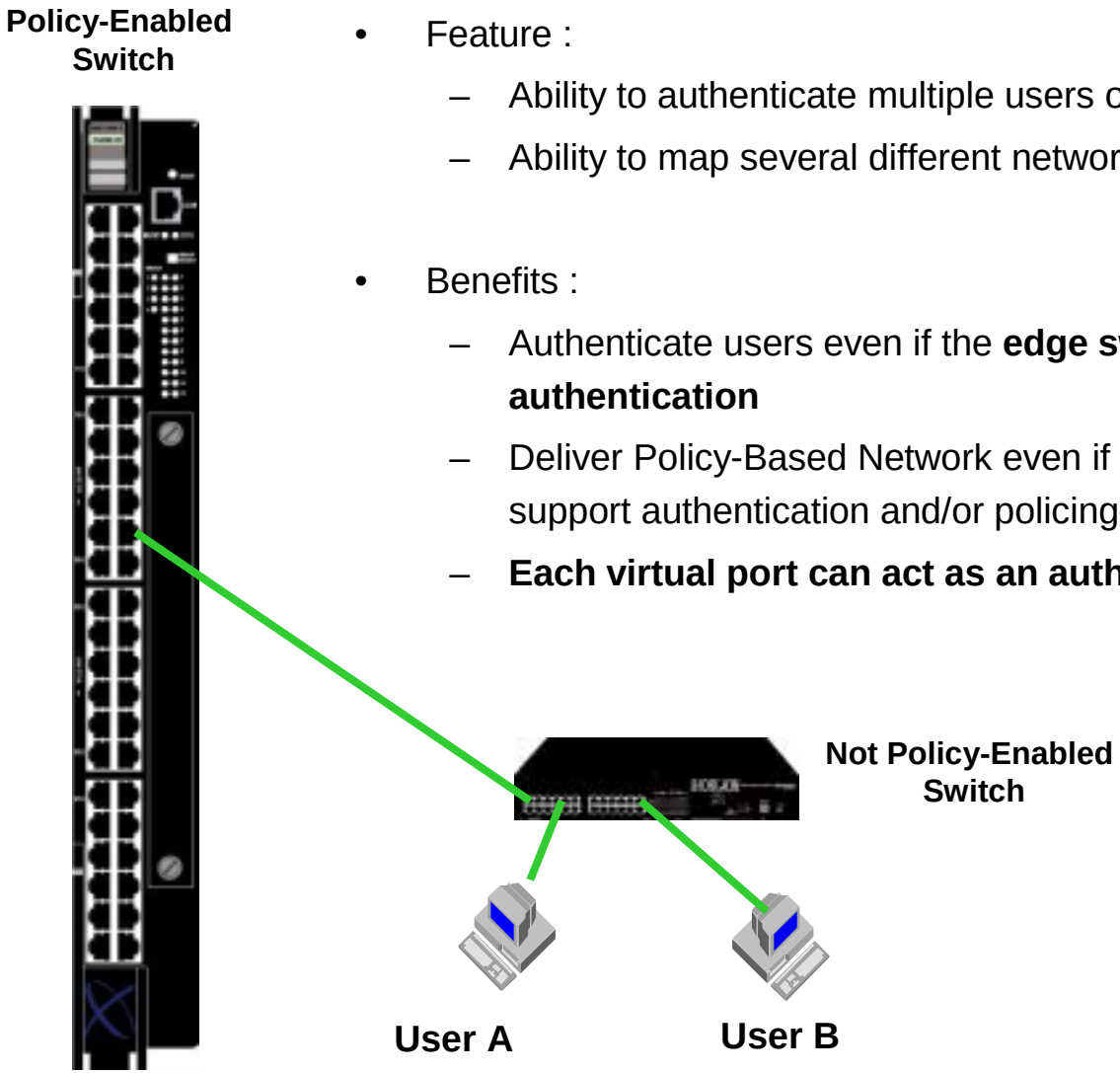
- Rapid response to security threats
- L2/L3/L4 granular control per user/port
- Filtering, VLAN assignment, QoS, Rate Limiting
- Simple, quick to implement

# Multi-user Authentication/Policy

**Allow multiple users (or devices) to authenticate via 802.1X, MAC-based, or Web-based (PWA) on a single port**



# Multi-User Authentication




- Feature :
  - Ability to authenticate multiple users on a single port
  - Ability to map several different network policies (profiles) on a port
- Benefits :
  - Authenticate users even if the **edge switches do not support authentication**
  - Deliver Policy-Based Network even if the edge switches do not support authentication and/or policing **(Virtual Ports/physical port)**
  - **Each virtual port can act as an authentication point**

# VLAN Assignment via User Authentication

- IEEE 802.1X RADIUS
- RFC 3580 defines how RADIUS attributes are to be used in an 802.1X context
- The main RADIUS Attributes of interest are: NAS-IP-Address, NAS-Port, NAS-Port-Type, Calling-Station-Id and Tunnel Attributes
- For use in VLAN assignment, the following RADIUS Tunnel Attributes are used:
  - **Tunnel-Type=VLAN (13)**
  - **Tunnel-Medium-Type=802**
  - **Tunnel-Private-Group-ID=VLANID**

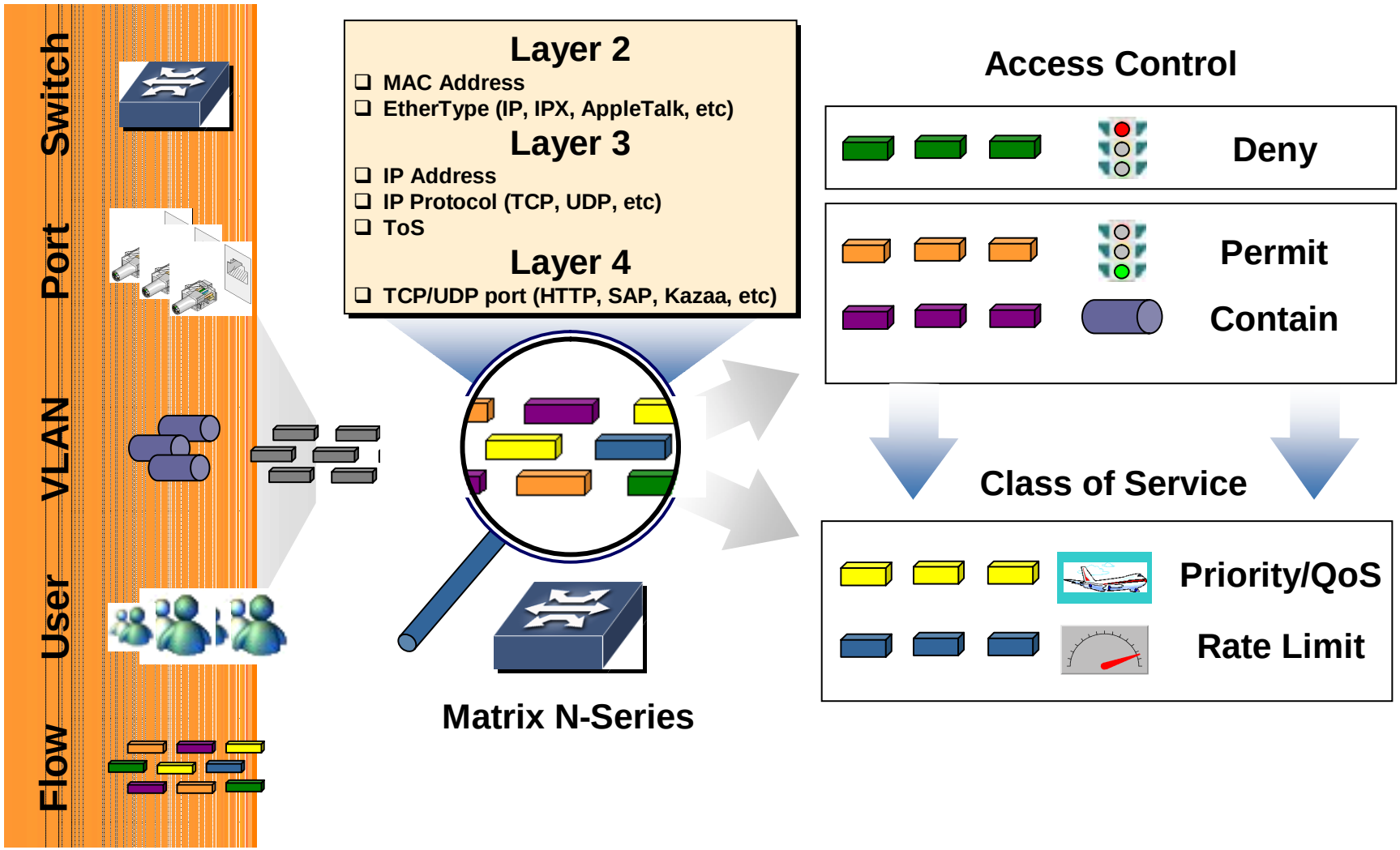
- Not a Policy Architecture, but allows non-policy enabled edge devices to be integrated in a policy rich environment (VLAN-to-Policy mapping)

# Enhanced Policy in a RFC 3580 Environment

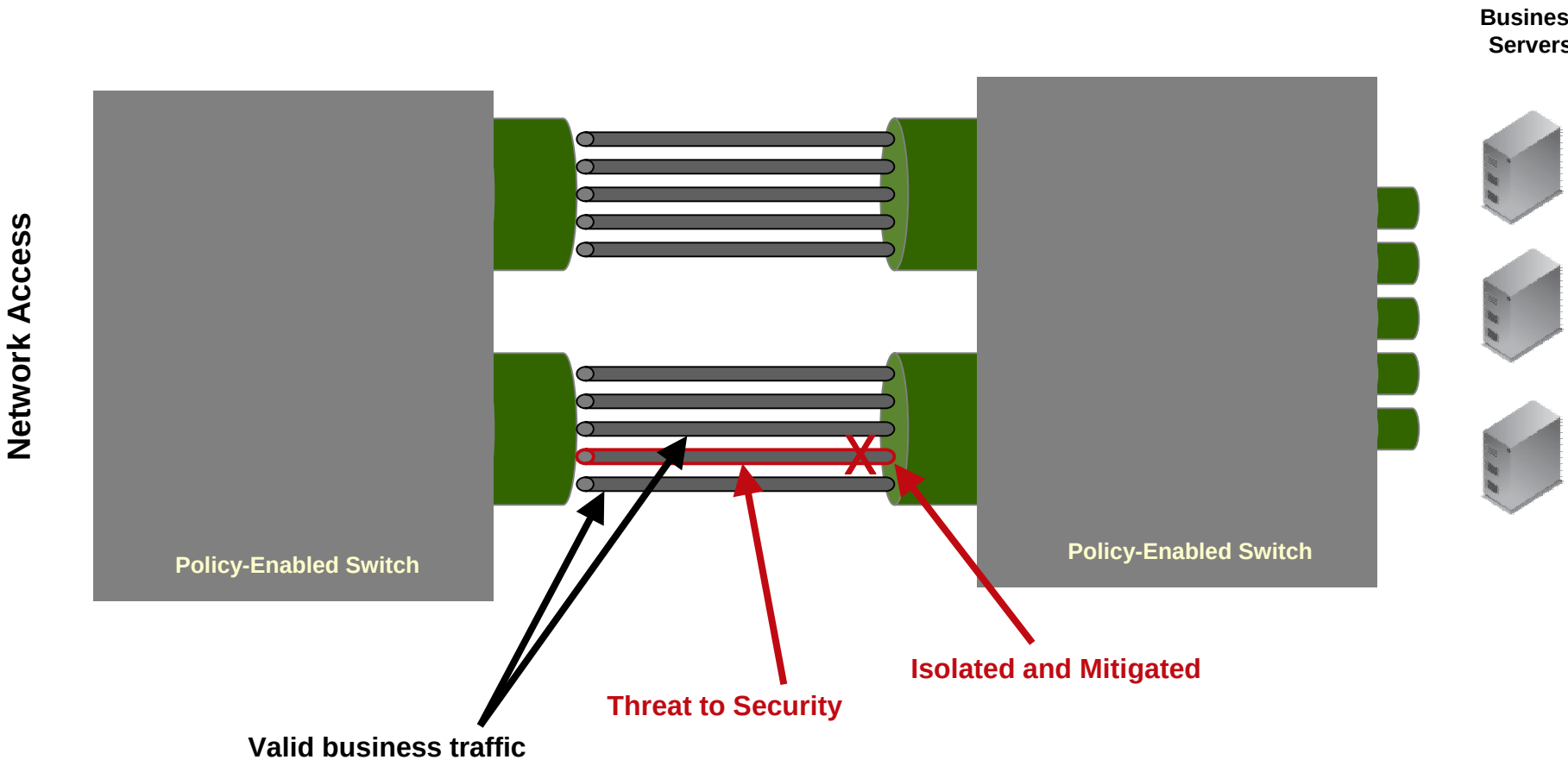
- Not policy-enabled access switches
- Leverage the VLAN ID as an indicator of the policy Role of the authenticated user
- Enforce policy Rules using new **“VLAN-to-Policy Mapping”** feature

- VLAN IDs are mapped to Policy IDs
- VLAN ID is assigned upon user authentication at the port level in network edge switch supporting RFC 3580
- Tagged (802.1Q) traffic is forwarded to the distribution level via 802.1Q trunks
- Inbound 802.1Q tagged traffic is handled at the distribution level by which is using the VLAN ID contained in the 802.1Q tag to map it to the associated Policy ID (Role)

# Dynamic Flow-based Packet Classification

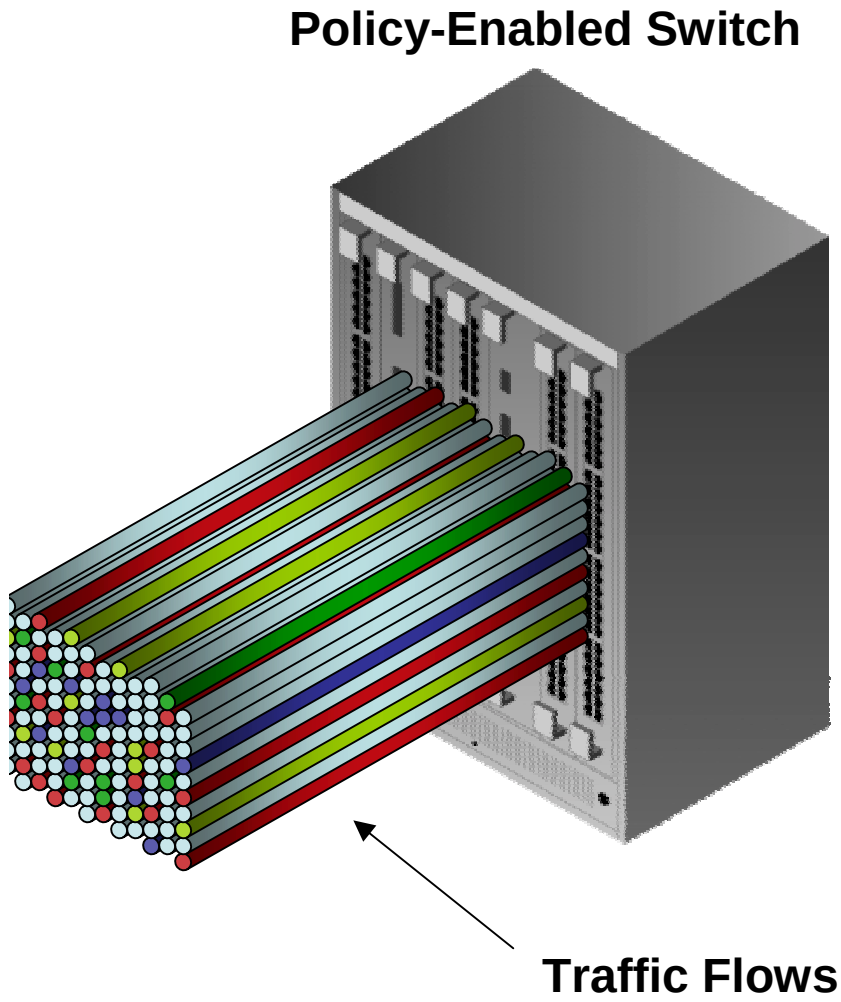


# Flow-Based architecture

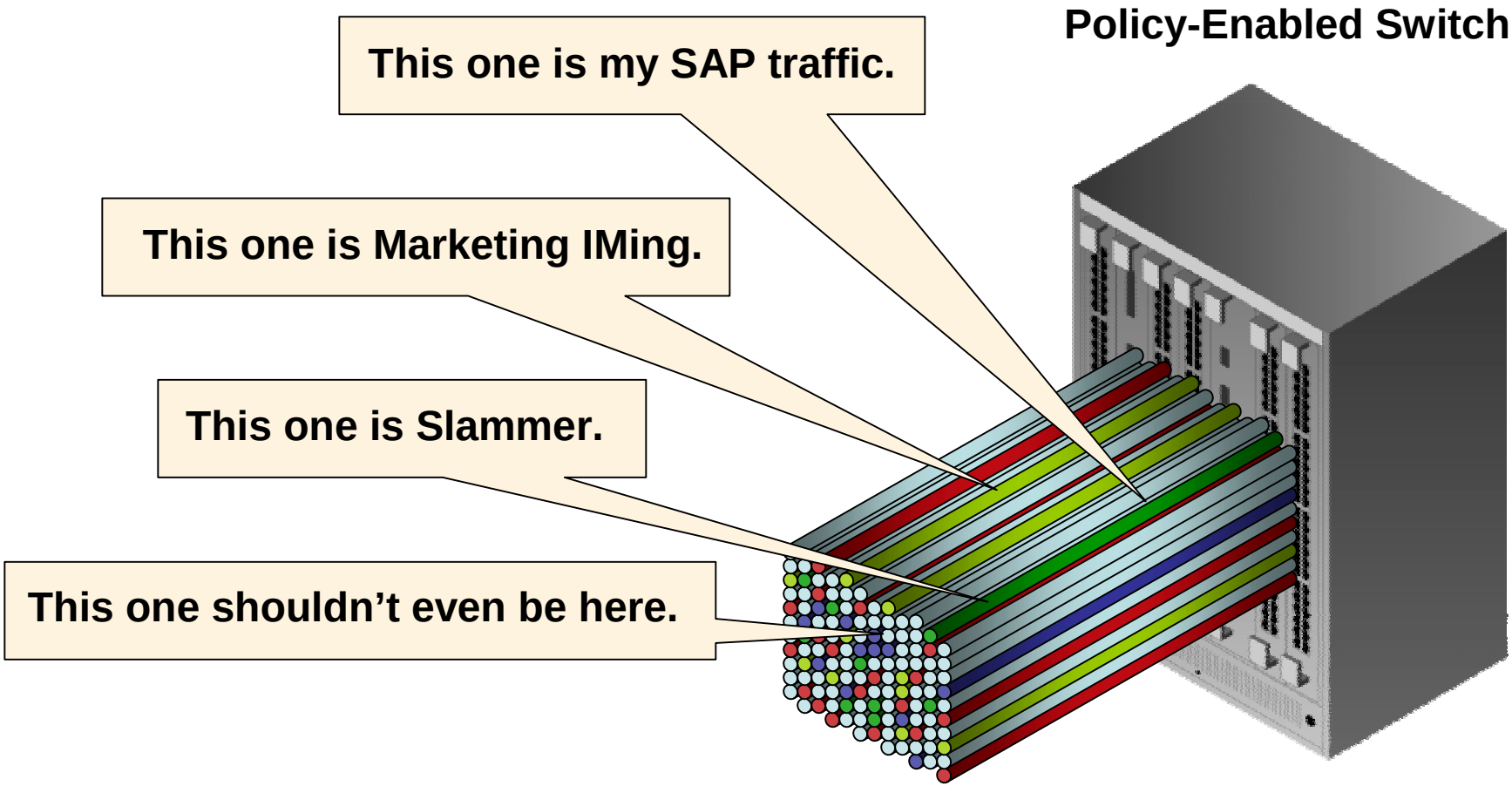


# Distributed Flow-Based Switching

- **Distributed Flow-based Switching:**
  **Provides enough bandwidth and processing power to meet demand**
  - **Traffic flows are analyzed as they enter the network**
    - Rules are then applied and action is determined
    - All frames in a flow are treated the same way
    - New flow is identified only if flow changes
- **Advantages**:
  - Each blade in a chassis has it's own dedicated processing power
    - Up to 100,000 flow setups/module
    - Helps maximize performance while maintaining granularity and control of traffic
  - **No single point of failure**
  - **Flow Setup Throttling allows granular control over spikes in flows caused by network threats**



# Distributed Flow-Based Switching




**Supports up to 100,000 flow setups/sec per interface module (up to 700,000 flow setups/sec per chassis)**

# Flow Setup Throttling

- **Flow Setup Throttling allows the network administrator to define an appropriate number of acceptable flows per port as well as monitor the new flow arrival rate.**
  - Flow Setup Throttling directly combats the effects of Denial of Service (DoS and DDoS) attacks by allowing the network administrator to limit the number of new or established flows that can be created on any individual switch port.
  - Denial of Service (DoS) attacks on the network generate a large amount traffic in a very short period of time which blocks the normal enterprise traffic. Uncontrolled, Denial of Service (DoS) attacks can essentially paralyze the entire enterprise network in a matter of minutes.
  - The ability to generate SNMP Notifications can be globally controlled on the switch.

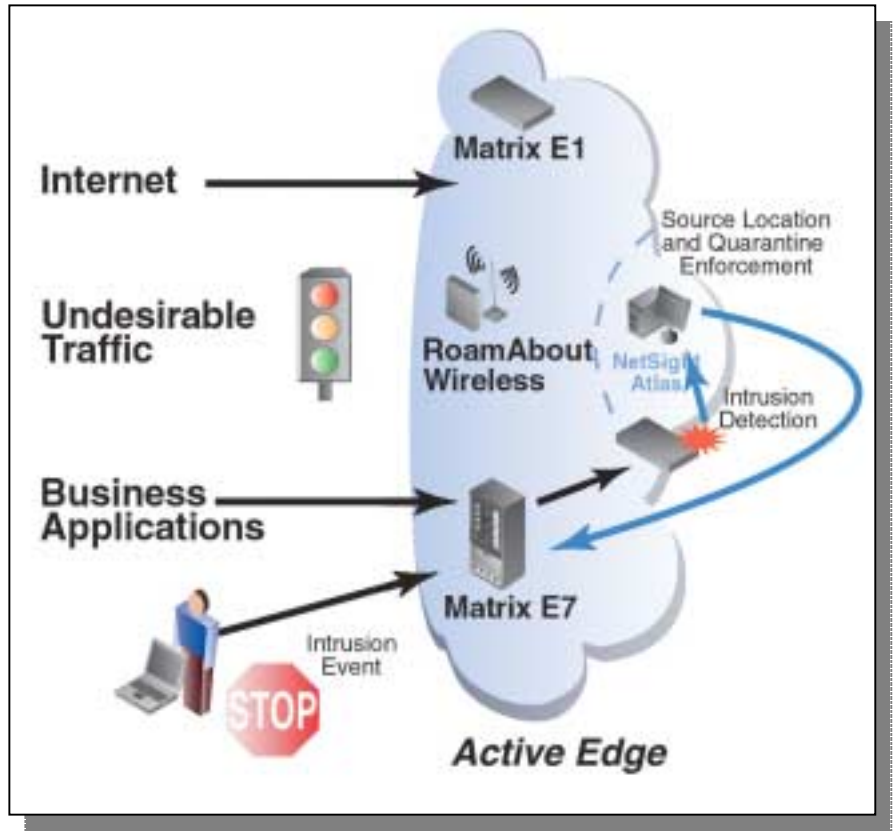
| Class | ActionLimit 1 | ActionTaken1 | ActionLimit2 | ActionTaken2 |
|---|---|---|---|---|
| User Port | 800 | generateNotification | 1000 | generateNotification, disableInterface |
| Server port | 5000 | generateNotification | 6000 | generateNotification, disableInterface |
| Aggregated User Port | 5000 | generateNotification | 6000 | generateNotification, disableInterface |
| InterSwitch Link | 14000 | generateNotificatio | 16000 | generateNotification |

# Span Guard

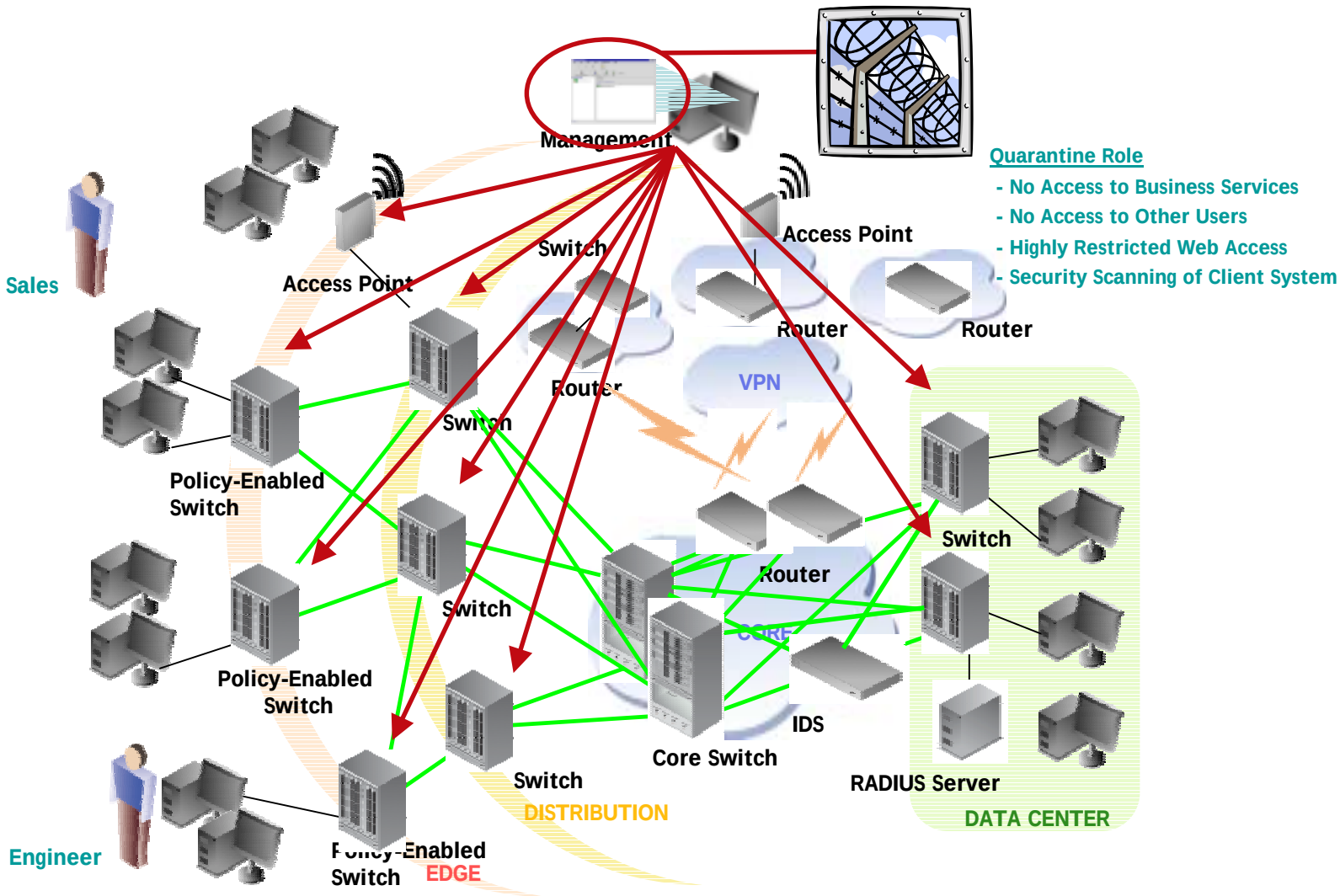
- **Restrict BPDUs on ‘user’ ports**
  - Typically there is no reason a BPDU should show up on a user port
    - Enabling "Span Guard" on "user" ports blocks Spanning Tree protocols and also provides notification through network management that a Spanning Tree protocol was detected.
  - Reception of a BPDU (except loop back) by a port, causes the port to be locked and its state set to "blocking"
    - Port will be locked for a globally specified time (*spanguardtimeout*) expressed in seconds,
      - Port can be locked indefinitely when timer value is set to 0.
    - Port will become unlocked
      - When the timer expires, or is manually unlocked, feature is disabled
  - Spanguard is used to prevent an attacker from injecting superior BPDUs into the network in an attempt to cause network topology changes.
  - If Spanguard is not enabled, such an attack will cause re-spanning issues that could cause a significant loss of availability of critical services on the network as ports are sent into blocking, MAC address tables are flushed, and high rates of flooded traffic are seen on the network.

# Dynamic Intrusion Response

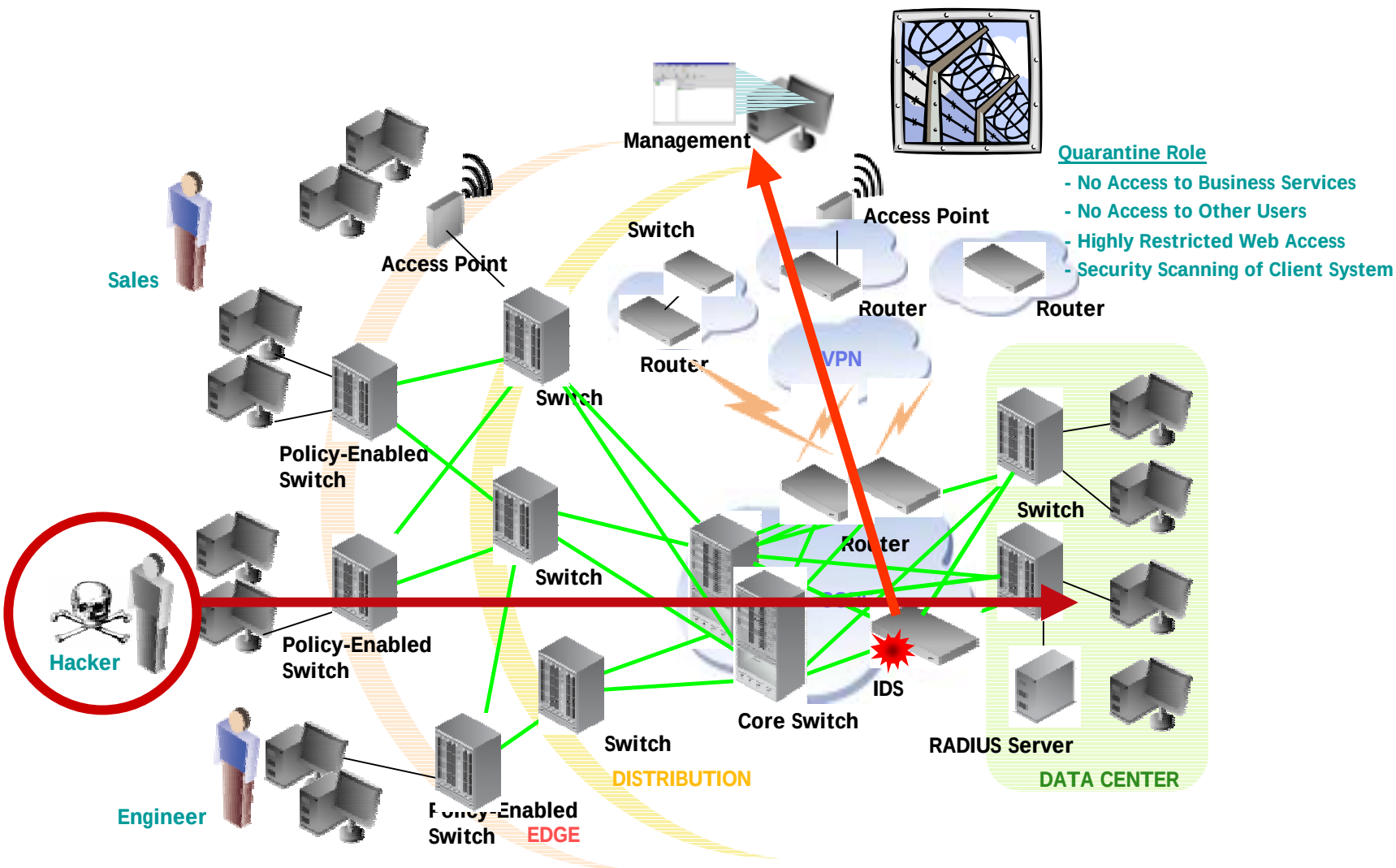
- **Centrally administered network usage policy**
  - Acceptable Use Policy
  - Organizational security and resource usage policy
- **Threat Containment Strategy**
  - Pre-defined highly secure policy Role (“Quarantine”)
  - Configurable for appropriate minimal services
- **Threat Detection**
  - Intrusion Detection System
  - Shared event log identifying threat
- **Location Services**
  - Source location tool
- **Automated Response**
  - Pre-defined custom response
  - Automated assignment of Containment policy (“Quarantine”) to located threat source



# Quarantine Policy



# Intrusion Detection : Detect



# NodeAlias to Locate users

Node aliases are dynamically assigned upon packet reception to ports

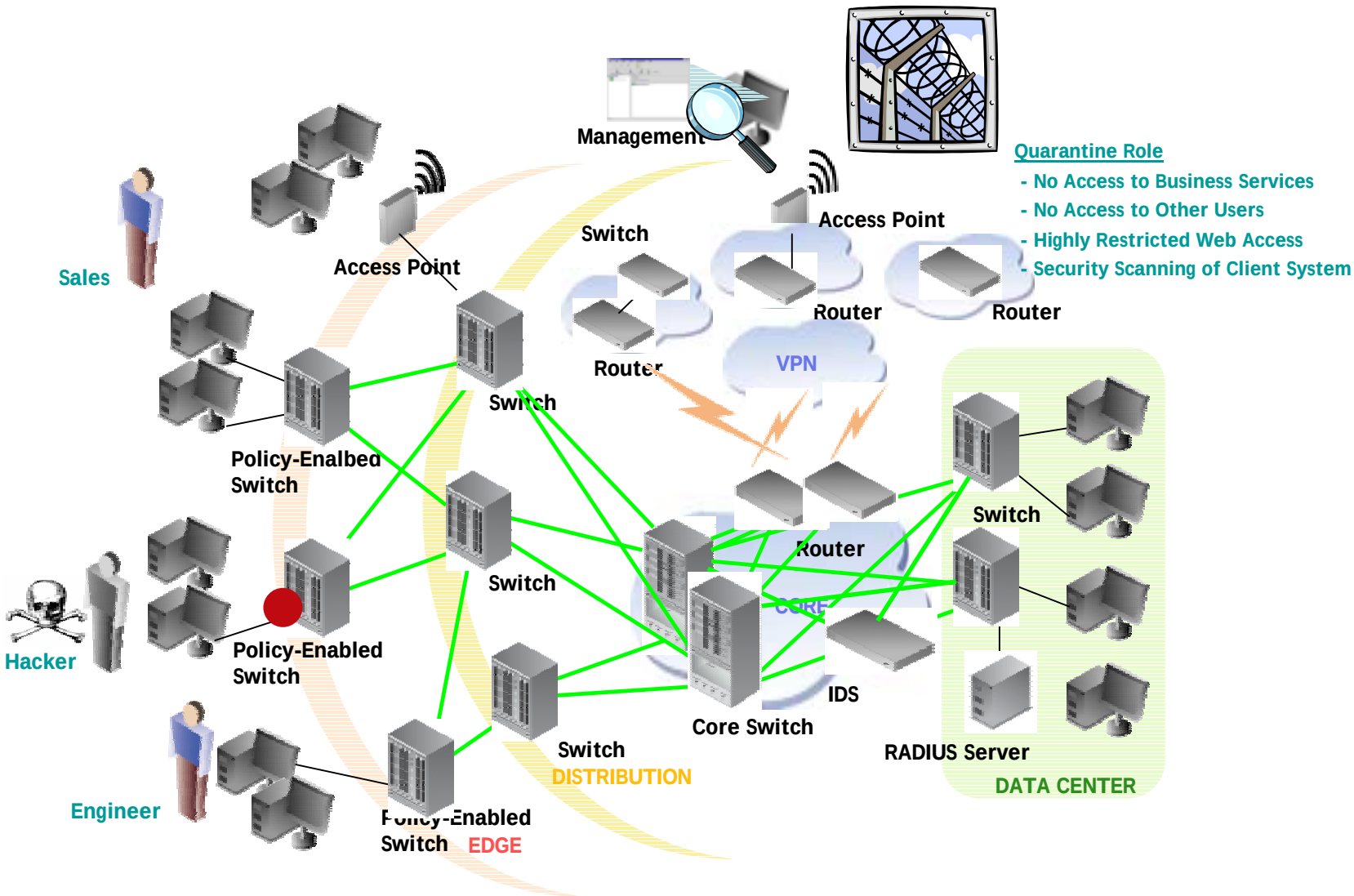
- The passive accumulation of a network's Node/Alias information is accomplished by "snooping" on the contents of network traffic as it passes through the switch fabric

- Vlan ID : VLAN ID associated with this alias.
- MAC Address : MAC address associated with this alias.
- Protocol : Networking protocol running on this port.
- Address / Source IP : When applicable, a protocol-specific address associated withthis alias.

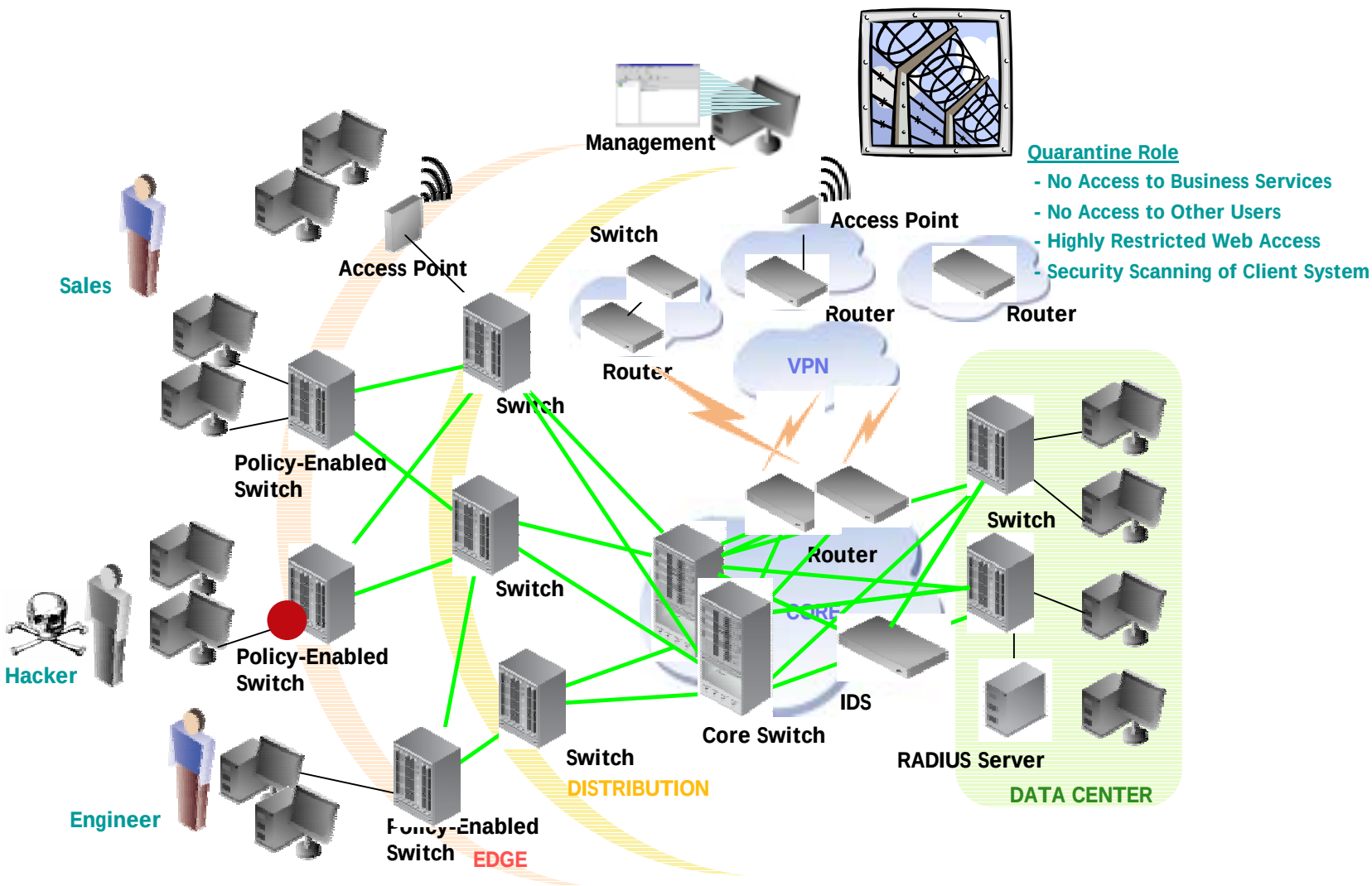
```
Matrix(rw)->show nodealias ge.3.12

Alias ID       = 1533917044          Active      = true
Vlan ID        = 1                   MAC Address = 00-e0-63-04-7b-00
Protocol       = ip                  Source IP = 63.214.44.63
```

# Intrusion Detection: Locate



# Intrusion Detection: Respond and Correct



# Una via per aggiungere valore al business aziendale

Una visione “olistica” della rete, la rete è vista in quanto  totalità organizzata e non in quanto semplice somma di  parti indipendenti tra loro (FW,VPN,IDS,..)
Il risultato è una Rete Sicura in senso olistico, ovvero che integra la sicurezza in tutta l’infrastruttura aziendale, garantendo protezione dalla periferia al core.
La RETE non è più soltanto vista con un focus su connettività e capacità ma deve considerarsi una via per aggiungere valore al business.
(*Business-Driven-Network*)


Mauro Rossi
SevenOne Solution