Rede Segura - UNIVATES

Centro Universitário UNIVATES

Lajeado – RS

Luis Antônio Schneiders

A UNIVATES

- Laboratórios, museus e salas especiais: 107
- Número de alunos:
  - Graduação: 7.398
  - Técnicos: 872
  - Extensão: 929
  - Seqüenciais: 131
  - Pós-graduação (Especialização): 496
  - Pós-graduação (Mestrado): 56

A UNIVATES

- Número de funcionários: 411
- Número de professores: 406
- Número de cursos:
  - Extensão: 49
  - Técnicos: 09
  - Seqüenciais: 02
  - Graduação: 37
  - Pós-Graduação (Especialização): 16
  - Pós-Graduação (Mestrado): 01
- Programas/Projetos de Extensão: 17
- Projetos de Pesquisas: 40

Equipamentos da Rede UNIVATES

- 15 switches VH
- 19 switches V2
- 02 switches A2
- 02 switches B2
- 01 N7 (2 DFEs platinum)
- 09 switches C2
- 02 routers CISCO
- Cabeamento estruturado em todos os prédios
- 10 prédios interligados por fibra (Gbps)

Clientes da Rede UNIVATES

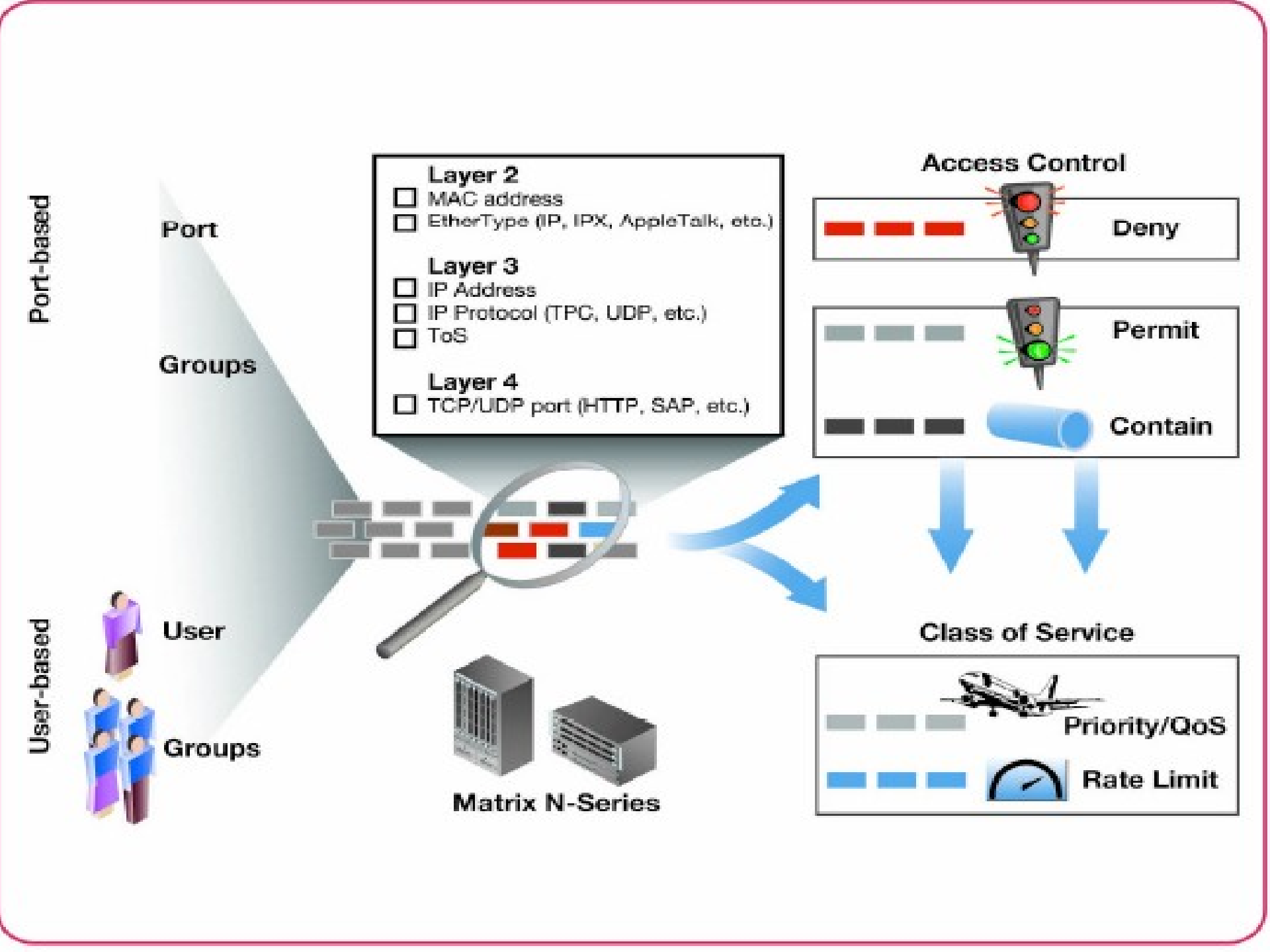
- Alunos
  - Regulares
  - Egressos
  - Visitantes
- Professores
  - Horistas
  - Visitantes
  - Tempo Contínuo
- Área Administrativa
- Empresas e serviços terceirizados
- Comunidade (GUEST)

Sem a implantação da Rede Segura

- Necessidade de pré-configuração de cada ponto de rede
- Problemas de acesso e segurança:
  - possibilidade acesso físico indevido a algum ponto pré-configurado disponível;
  - problemas na identificação do usuário conectado;
  - Distribuição estática de VLANs.

Situação Desejada

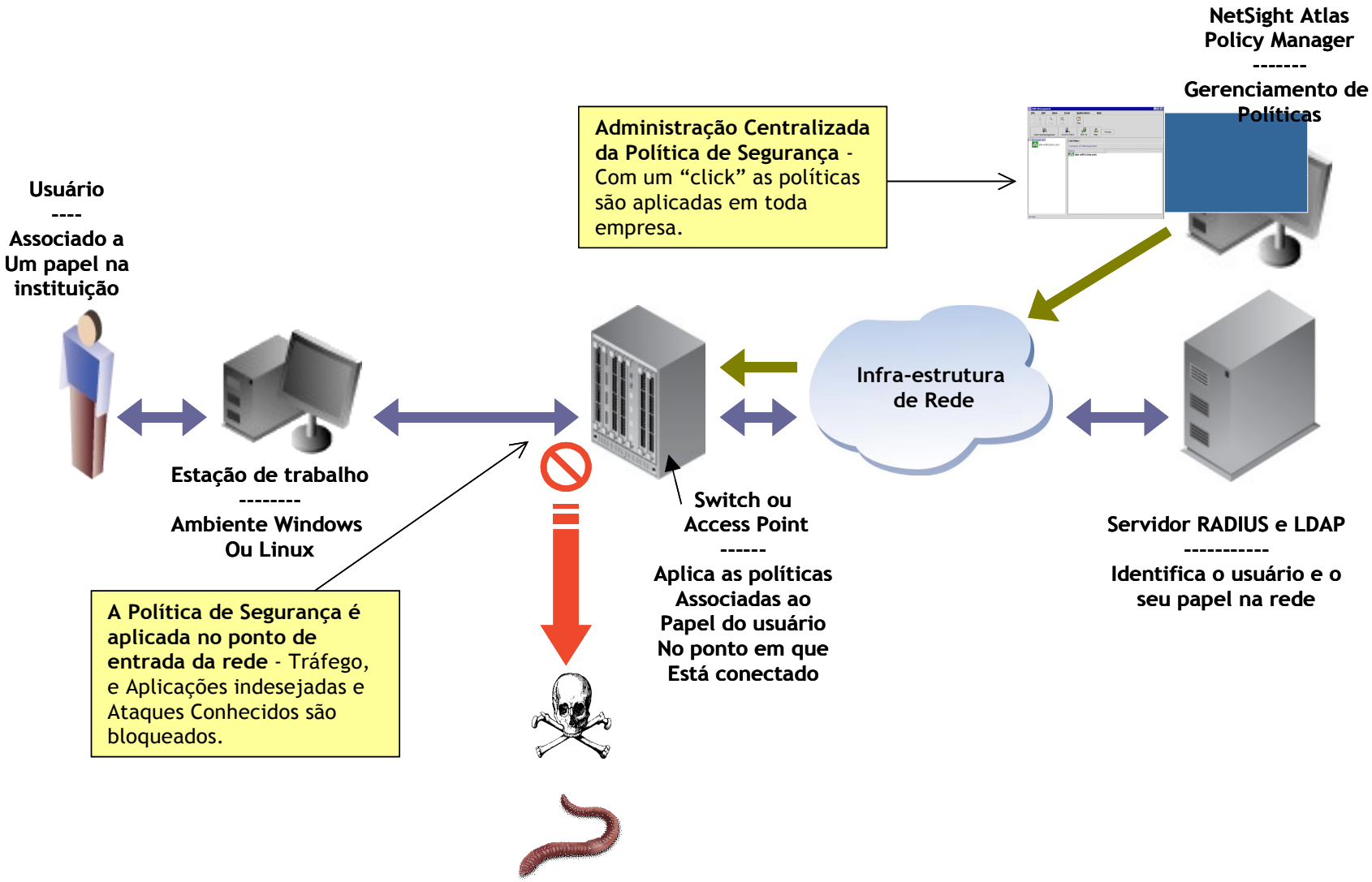
- Identificação e autenticação de todos os usuários da Rede Univates no momento da sua conexão;
- Implantação de políticas de acesso à rede de acordo com o papel de cada usuário;
- O usuário ter acesso a todos os seus dados e privilégios a partir de qualquer ponto da rede;
- Evitar a utilização não autorizada da rede;
- Controlar usuários visitantes.


Port-based
Port
Groups
User-based
User
Groups
Layer 2
MAC address
EtherType (IP, IPX, AppleTalk, etc.)
Layer 3
IP Address
IP Protocol (TPC, UDP, etc.)
ToS
Layer 4
TCP/UDP port (HTTP, SAP, etc.)
Matrix N-Series
Access Control
Deny
Permit
Contain
Class of Service
Priority/QoS
Rate Limit

IEEE 802.1x

- **O padrão requer**
  - **uma infra-estrutura de suporte**
  - **clientes nominais que suportem o 802.1X**
  - **switches que podem participar no 802.1X**
  - **um servidor RADIUS**
  - **algum tipo de banco de dados de contas (como o Active Directory - LDAP).**

Situação Desejada



Modelos Possíveis

Modelo Acceptable Use Policy (AUP) - Implementando a política de segurança

Este modelo aplica uma política de segurança e qualidade de serviço persistente a todos os usuários e dispositivos que se conectam à rede sem necessidade de autenticação.

Modelo Secure Application Provisioning (SAP) - Personalizando segurança e qualidade de serviço

Permite a personalização da política de segurança e qualidade de serviço de acordo com o perfil do usuário autenticado.

Modelo Secure Guest Access (SGA) - Controlando acesso de visitantes

Permite definir políticas de acesso limitado para visitantes. Exemplo de política de visitante: acesso limitado apenas à Internet (http) com limitação de largura de banda de 128Kbps.

Modelo Dynamic Intrusion Response (DIR) - Respondendo automaticamente a ataques

Este modelo integra o IDS – sistema de detecção de intrusos - com as políticas da rede através do console de gerenciamento de segurança NetSight Automated Security Manager, capaz de localizar precisamente a origem de um ataque em tempo real (switch e porta) e aplicar uma política de quarentena adequada ao nível de criticidade do evento.

Modelo adotado na UNIVATES

Modelo Acceptable Use Policy (AUP) - Implementando a política de segurança

Este modelo aplica uma política de segurança e qualidade de serviço persistente a todos os usuários e dispositivos que se conectam à rede sem necessidade de autenticação.

Modelo Secure Application Provisioning (SAP) - Personalizando segurança e qualidade de serviço

Permite a personalização da política de segurança e qualidade de serviço de acordo com o perfil do usuário autenticado.

Modelo Secure Guest Access (SGA) - Controlando acesso de visitantes

Permite definir políticas de acesso limitado para visitantes. Exemplo de política de visitante: acesso limitado apenas à Internet (http) com limitação de largura de banda de 128Kbps.

Modelo Dynamic Intrusion Response (DIR) - Respondendo automaticamente a ataques

Este modelo integra o IDS – sistema de detecção de intrusos - com as políticas da rede através do console de gerenciamento de segurança NetSight Automated Security Manager, capaz de localizar precisamente a origem de um ataque em tempo real (switch e porta) e aplicar uma política de quarentena adequada ao nível de criticidade do evento.

Metodologia de implantação

- Definição do nível de segurança adotado (SGA-SAP) utilizando autenticação EAP TTLS;
- Definição e documentação dos papés dos usuários e dos seus perfis de acesso;
- Identificação das vulnerabilidades;
- Disponibilização da equipe de implantação;
- Disponibilização de equipamentos para a criação da base de testes;
- Implantação definitiva após aprovação dos testes.

Características da UNIVATES

- Utilização de software livre nos servidores e na maioria das estações de trabalho;
- Necessidade de convivência das estações de trabalho windows e linux no processo;
- Alunos, professores e demais usuários com notebooks (necessidades distintas de acesso);
- Utilização do FreeRADIUS e OpenLDAP;
- Utilização do SAMBA para criação de diretório HOME dos usuários windows.

Configurando o Ambiente

- Estações clientes
  - Cliente Windows (SecureW2)
  - Cliente Linux (xsupplicant)
    - Necessitou de desenvolvimento de um módulo em c para integração da tela de login do ambiente gráfico com o PAM (sistema de autenticação)
    - Senhas MD-5

Configurando o Ambiente

- Servidor Linux (RedHat 5)
  - OpenLDAP
    - Reestruturação da árvore para acomodar os papéis (atributos) dos usuários
  - FreeRADIUS
    - Uso de TTLS
    - Certificado assinado por entidade certificadora válida
    - Protocolo de autenticação MS-CHAPv2

Situação Atual

Clientes windows

- Sem autenticar o usuário não possui acesso algum a rede.
- Depois de autenticado seu acesso é restrito as regras relacionadas a seu papel

- Clientes Linux
  - É necessário uma política que permita um acesso mínimo a rede para verificar o usuário na base antes de autenticar. Isso obriga a disponibilizar um acesso mínimo e um domínio pré-configurado

Obrigado