

TÓPICOS ESPECIAIS EM DEFESA CIBERNÉTICA

Professor Me. Vladimir Geraseev Junior

**Curso: TECNOLOGIA EM DEFESA
CIBERNÉTICA**

**Disciplina: Tópicos Especiais em Defesa
Cibernética**

Sejam Bem Vindos!

Prof. Vladimir Geraseev Junior

PROF VLADIMIR GERASEEV JUNIOR

- **GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO**
- **MESTRADO EM ENGENHARIA - UNITAU**
- **EXPERIÊNCIA PROFISSIONAL:**
 - COMPANHIA DE INFORMÁTICA DE JUNDIAÍ – ARQUITETO DE REDES
 - EMBRAER – GRUPO DE ENGENHARIA
 - INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS – INPE – ANALISTA DE REDES E SEGURANÇA
 - IMPLEMENTAÇÃO DOS REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES (ATO 77) – ANATEL
 - CONSULTORIA EM CONDUÇÃO DE PENTESTS

PROF VLADIMIR GERASEEV JUNIOR

- EXPERIÊNCIA PROFISSIONAL ACADÊMICA.
- PROFESSOR NA FATEC TAUBATÉ
- PROFESSOR NA ETEC JACAREÍ
- PROFESSOR EM UNIVERSIDADES PARTICULARES (UNIP, UNIVAP, FAPI)

- NEXT GENERATION
FIREWALLS

O FIREWALL TRADICIONAL JÁ NÃO É SUFICIENTE

Firewalls tradicionais bloqueiam apenas endereços IP e Portas
Muitas aplicações atuais utilizam portas 80 e 443 (HTTP e HTTPS)
Firewalls Tradicionais não podem examinar estas aplicações



Next Gen firewalls usam Inspeção Profunda de Pacotes
Conseguem identificar as aplicações que usam portas 80 e 443
Verificação completa do tráfego incluindo IPS, Antivírus e Filtro Web

CONTROLE E INTELIGÊNCIA DE APLICAÇÕES

Identifica Milhares de Aplicações pela Assinatura e não pela porta

Permite Controle muito mais Efetivo que Firewalls Tradicionais

Pode-se criar políticas por:

Grupos de aplicações, aplicações ou mesmo componentes de uma aplicação

Grupos de usuários ou usuários

Hora do Dia

IP, Endereço MAC

Categoria de Site ou URL

corp/jsilva



Integração com LDAP,
Active Directory e Radius



Banco de Dados de Aplicações e Sites constantemente atualizado

1ª: CONTROLAR APLICAÇÕES PERMITIDAS NA REDE

Deseja garantir que todos estejam com a ultima versão do Internet Explorer? Crie uma política que redireciona usuários de versões antigas para uma pagina de Download.

Outros exemplos:



Skype permitido somente para a Diretoria

Dropbox permitido durante Horário Comercial

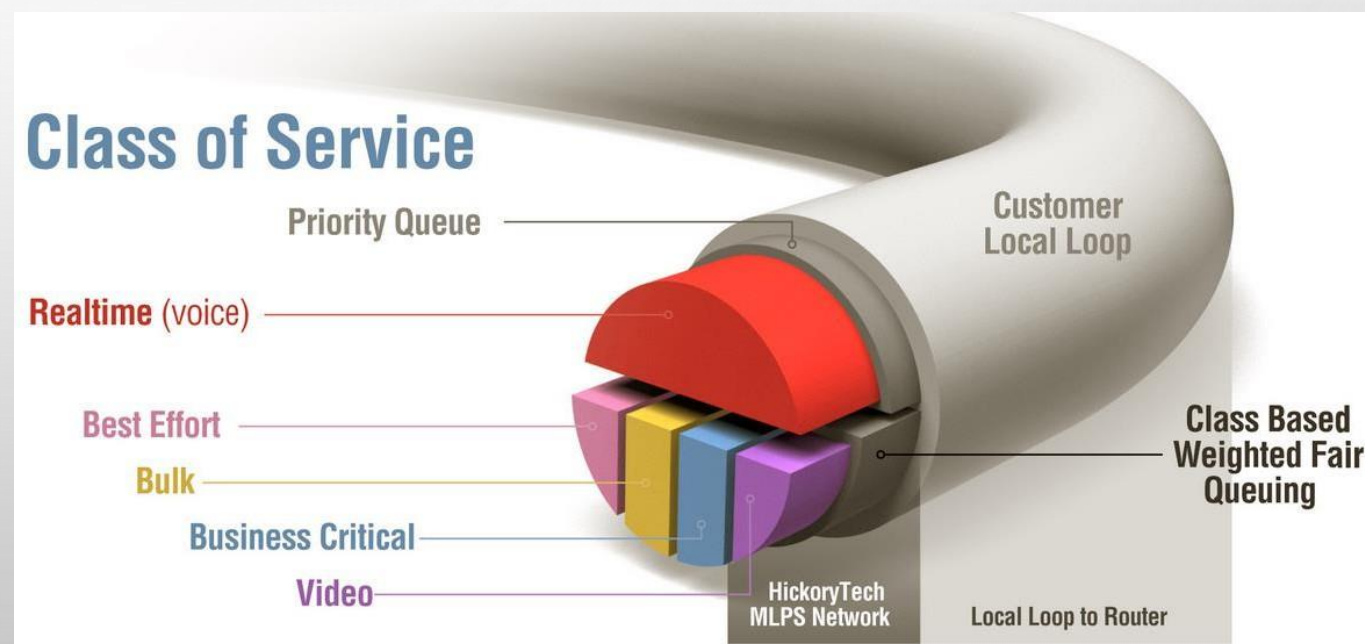
WhatsApp permitido somente para Vendas



2ª: PRIORIZAR APLICAÇÕES E SITES DE NEGÓCIOS

Aplicações Críticas como Salesforce.com, Office365, Webinários e VoIP, baseadas em nuvem ou executadas sobre uma WAN devem ter prioridade sobre outras aplicações como navegação comum.

Pode-se criar políticas granulares para priorizar aplicações, origem, destino, grupo de usuários ou URLs.

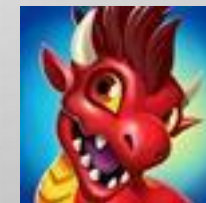


3ª: BLOQUEAR APLICAÇÕES IMPRODUTIVAS



4ª: BLOQUEAR COMPONENTES NÃO PRODUTIVOS

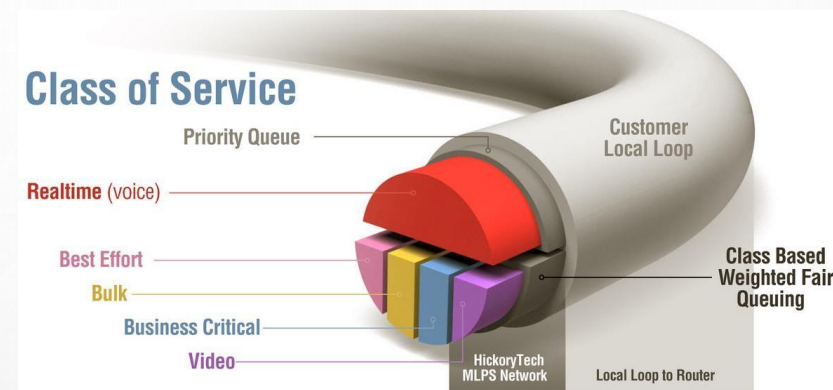
- APLICAÇÕES DE REDES SOCIAIS COMO FACEBOOK, TWITTER E YOUTUBE
 - SÃO UTILIZADAS COMO MEIOS DE COMUNICAÇÃO EM EMPRESAS.
 - PARA ALGUNS GRUPOS DE USUÁRIOS PODE SER CONTRA PRODUTIVO
- BLOQUEAR ESTAS APLICAÇÕES, PORÉM PODE-SE CONTROLAR COMO ESTAS APLICAÇÕES SÃO UTILIZADAS BLOQUEANDO-SE, POR EXEMPLOS, AS APLICAÇÕES DO FACEBOOK COMO CANDY CRUSH, FARMVILLE 2, DRAGON CITY, WORDS WITH FRIENDS, ETC.



5ª: GERENCIAR A BANDA PARA UM GRUPO

A produtividade pode ser afetada se houver uma política restritiva de acesso a aplicações Web. Opcionalmente pode-se permitir acesso com banda reduzida para determinados grupos de usuários enquanto que a diretoria é mantida com a banda normal.

Pode-se escolher grupos do Ad, associar a grupos de Aplicações e definir políticas nos dois casos acima.



6ª: BLOQUEAR A ENTRADA DE VÍRUS NA REDE

Bloqueio de vírus só no Endpoint pode colocar em risco sua rede. Nem sempre pode-se garantir que todos os Endpoint estejam com antivírus ativo e atualizado.

Nestes casos é importante ter uma camada adicional de antivírus no gateway de sua rede.



Os Next Generation Firewalls possuem tecnologia para identificar Virus, Keyloggers, Spyware, Trojans e outras tentativas de Intrusão via Web, E-mail, FTP, IM, etc. com um mínimo de latência.

7ª: IDENTIFICAR CONEXÕES POR PAÍS

A conexão é para um endereço IP de outro país? Que aplicações estão tentando acessar IPs de quais países?

Pode-se criar filtros baseados em endereços de outros países para se aumentar a proteção ou restringir o acesso.



8ª: GERENCIAR BANDA DE ÁUDIO E VÍDEO

- ACESSO A STREAMING VÍDEO COMO YOUTUBE PODE SER PRODUTIVO EM
- ALGUNS CASOS, MAS TAMBÉM PODE SER ABUSIVO.
- ESTES TRÁFEGOS PODEM VIR DE SITES NÃO RELACIONADOS, COMO POR
- EXEMPLO UM VÍDEO INSERIDO EM UM BLOG.
- PODE-SE CRIAR POLÍTICAS DE APLICAÇÕES COM FOCO EM STREAMING PARA LIMITAR O CONSUMO DE BANDA.
- PODE-SE AINDA APLICAR ESTA RESTRIÇÃO PARA APENAS O HORÁRIO COMERCIAL.